

Arithmetic of Algebraic Groups

A thesis in Mathematics by
Shripad M. Garge

under the guidance of
Professor Dipendra Prasad

submitted to the
University of Allahabad

in partial fulfillment of the requirements for
the degree of
Doctor of Philosophy

Harish-Chandra Research Institute, Allahabad.
2004

Certificate

This is to certify that the D.Phil. thesis titled “Arithmetic of algebraic groups” submitted by Shripad M. Garge is a bonafide research work done under my supervision. The research work present in this thesis has not formed the basis for the award to the candidate of any degree, diploma or other similar titles.

Harish-Chandra Research Institute
Allahabad. India.

Prof. Dipendra Prasad
Thesis Supervisor.

Date:

Acknowledgments

This thesis would not have been written without the support and encouragement of several friends and well-wishers. It is a great pleasure for me to acknowledge them. I may not be able to list all individually, but I hope that they will recognize themselves and find my warmest thanks here.

First and foremost I would like to thank my thesis supervisor, Prof. Dipendra Prasad. It is with a deep sense of gratitude that I acknowledge the help and the constant support I have received from him. The questions studied in this thesis are formulated by him. I have immensely benefited from discussions with him. My mathematical training is based more on discussions with him than on formal courses. He trusted my ability and was patient enough to explain some very basic things to me.

I am grateful to Dr. Maneesh Thakur for encouragement and constant help. He was always ready to discuss with me, to listen to my naive (and many times wrong) ideas and to correct me without making me feel bad about it. I am grateful to him for running a seminar on ‘central simple algebras and Brauer groups’ which helped me a lot in the understanding of linear algebraic groups. I owe much more to him than I can write here.

I was lucky to have been able to discuss with many renowned mathematicians. I would like to thank them for their kind words of encouragement and support. In particular, I would like to thank Prof. M. S. Raghunathan, Prof. Gopal Prasad, Prof. R. Parimala, Prof. Madhav Nori, Prof. Mikhail Borovoi and Prof. Boris Kunyavskii. I would also like to thank Prof. J.-P. Serre and Prof. T. A. Springer for their encouraging correspondence.

I have had very helpful mathematical discussions with A. Raghuram, C. S. Rajan, Joost van Hamel, D. Surya Ramana, C. S. Dalawat and Anupam Kumar Singh. I am grateful to all of them. I am also grateful to Prof. Adhikari, Prof. Passi, Prof. Kulkarni, and all other mathematicians at the Harish-Chandra Research Institute (HRI) for the support that I received from them. I would like to thank the administrative staff of HRI for their cooperation, special thanks are due to Mr. Amit Roy and Ms. Seema Agrawal.

I am grateful to my teachers for developing and nurturing my interest in Mathematics. I would like to thank Prof. Katre, Prof. Athavale, Dr. Bhate, Dr. Waphare and Dr. Naik for the extra efforts that they put in for me.

I affectionately thank all my friends with whom I shared good times and bad times as well. I thank Vinay and Smita, Ajita, Acharya Sir, Sheth Sir, Smita and Swapnil, Sarika and Viraj, Alok, Meghraj, Himanee, Dhanashree and Nikhil, and Sachin for the help that I received from them. It would not have been possible for me to concentrate on my work without their help. I would like to thank Ms. Kulkarni, Mr. Gosavi and Mr. Sunil of Bhaskaracharya Pratishthana, Pune, for

their help in various matters. I thank all my friends at Allahabad and Mumbai for making my stay lively and enjoyable, special thanks are due to the HRI football club.

I thank my parents, brothers, sisters-in-law, Vaishnavi and Nachiket for their tremendous support, especially in moulding my life. It is not possible to express my gratitude towards them in words. Last but not the least, I thank Anuradha for her constant love, support and unwavering trust in me. She provided me a nice motivation for completing this work soon and was not cross with me when I took my own sweet time to complete it.

I dedicate this thesis to Anuradha and the rest of my family.

Mathematics as an expression of the human mind reflects the active will, the contemplative reason, and the desire for aesthetic perfection. Its basic elements are logic and intuition, analysis and construction, generality and individuality. Though different traditions may emphasize different aspects, it is only the interplay of these antithetic forces and the struggle for their synthesis that constitute the life, usefulness, and supreme value of mathematical science.

Richard Courant and Herbert Robbins.
(What is Mathematics?)

Contents

Introduction	1
0.A. Maximal tori determining the algebraic group.	1
0.B. Orders of finite semisimple groups.	2
0.C. Excellence properties of F_4	5
0.D. General layout of the thesis.	5
Main results proved in this thesis	7
Chapter I. Linear algebraic groups	9
§1. Definition and basic properties.	9
§2. Structural properties of linear algebraic groups.	11
§3. Tori in reductive groups.	12
3.A. Maximal tori.	13
3.B. Weyl group.	13
3.C. Anisotropic kernel.	14
§4. Classification of simple algebraic groups.	14
4.A. Root system.	14
4.B. Classical split simple k -groups.	15
4.C. Exceptional split simple k -groups.	17
4.D. Non-split simple k -groups.	18
§5. Groups of type G_2 and F_4	18
5.A. Octonion algebras and groups of type G_2	18
5.B. Albert algebras and groups of type F_4	19
Chapter II. Galois Cohomology	21
§6. Basic definitions.	21
§7. Galois cohomology of linear algebraic groups.	22
7.A. Classification of k -forms.	22
7.B. $H^1(k, G)$ for some special fields k	24
§8. Galois cohomology and tori.	24
§9. Herbrand quotient.	26

Chapter III. Maximal tori determining the algebraic group	29
§10. Introduction.	29
§11. Galois cohomological lemmas.	30
§12. Reflection groups and characteristic polynomials.	33
§13. Determining the Weyl groups.	35
13.A. Exceptional group of rank m	36
13.B. The groups B_m and C_m	37
13.C. The group D_m	38
13.D. The group A_m	40
§14. Main result.	40
§15. Another proof of Theorem III.5.	43
Notes.	45
Chapter IV. Orders of finite semisimple groups	47
§16. Finite semisimple groups.	47
§17. Some preliminary lemmas.	48
§18. Determining the finite field.	49
18.A. Determining the characteristic of the finite field.	50
18.B. Determining the finite field.	54
§19. Pairs of order coincidence.	57
§20. On a group structure on pairs of order coincidence.	61
§21. A geometric reasoning.	64
Notes.	66
Chapter V. Excellence properties of F_4	67
§22. Excellence of linear algebraic groups.	67
§23. Albert algebras and groups of type F_4	68
§24. The main theorem.	70
Notes.	70
Bibliography	73
Index	77
Notation	79

Introduction

This thesis studies arithmetic of linear algebraic groups. It involves studying the properties of linear algebraic groups defined over global fields, local fields and finite fields, or more generally the study of the linear algebraic groups defined over the fields which admit arbitrary cyclic extensions.

We cover the basic material about linear algebraic groups in the first chapter. After defining a linear algebraic group in the first section, we introduce the notions of tori, reductive groups, semisimple groups and the simple algebraic groups. Since a reductive algebraic group admits an almost direct decomposition into simple algebraic groups and a torus, it is necessary to study simple groups and tori to understand the structure of reductive algebraic groups. We describe the classification of split simple algebraic groups using root systems. The description of non-split simple groups can be given using Galois cohomology, which is the main topic of the second chapter of this thesis.

One of the main applications of the Galois cohomology in the theory of the algebraic groups is to describe the forms of algebraic groups. Let G be an algebraic group defined over a field k . The k -groups H such that $H \otimes_k \bar{k}$ is isomorphic to $G \otimes_k \bar{k}$, where \bar{k} denotes the algebraic closure of k , are called as the k -forms of G . It is known that the set of the k -isomorphism classes of the k -forms of a group G is in bijection with the set $H^1(k, \text{Aut}_k(G))$ (Corollary II.3(1)). As a special case, we give the description of the k -isomorphism classes of n -dimensional tori defined over a field k . We also describe the k -conjugacy classes of maximal k -tori in a reductive group defined over a field k . After covering the preliminaries in the first two chapters, we report on author's research work in the next three chapters.

0.A. Maximal tori determining the algebraic group. We define an *arithmetic field* to be a number field, a local non-archimedean field or a finite field.

It is a natural question to ask if a connected reductive algebraic group defined over a field k is determined by the set of k -isomorphism classes of maximal tori contained in it. We study this question for split, semisimple groups defined over arithmetic fields, i.e, over number fields, local non-archimedean fields and finite fields. We prove that the Weyl group of a split, connected, semisimple k -group H , where k is an arithmetic field, is determined by the k -isomorphism classes of

the maximal tori in H . Since a split simple k -group is determined by its Weyl group, up to isogeny except for the groups of the type B_n and C_n , we get that the group H is determined up to isogeny except that we are not able to distinguish between the simple direct factors of H of the type B_n and C_n .

From the explicit description of maximal k -tori in SO_{2n+1} and Sp_{2n} , see for instance [21, Proposition 2], one finds that the groups SO_{2n+1} and Sp_{2n} contain the same set of k -isomorphism classes of maximal k -tori. We also show by an example that the existence of split tori in the group H is necessary.

We now give a brief description of the proof. Fix an arithmetic field k . The set of k -isomorphism classes of maximal tori in a reductive group H/k is in bijection with the equivalence classes of the integral Galois representations, $\rho : \mathrm{Gal}(\bar{k}/k) \rightarrow W(H)$, where $W(H)$ is the Weyl group of H . Now, let H_1, H_2 be reductive k -groups sharing the same set of maximal tori up to k -isomorphism. For a maximal torus $T_1 \subset H_1$, let $T_2 \subset H_2$ be a torus which is k -isomorphic to T_1 . Then the integral Galois representations associated to the tori T_i , say ρ_i , are equivalent (Lemma II.6). Hence the images $\rho_i(\mathrm{Gal}(\bar{k}/k)) \subset W(H_i)$ are conjugate in $\mathrm{GL}_n(\mathbb{Z})$. Next we prove that every cyclic subgroup of $W(H)$ appears as the image of a Galois representation associated to some maximal torus in H . Hence it follows that the Weyl groups $W(H_1)$ and $W(H_2)$ share the same set of elements up to conjugacy in $\mathrm{GL}_n(\mathbb{Z})$. Then the proof boils down to proving the following result:

If the Weyl groups of two split, connected, semisimple algebraic groups, $W(H_1)$ and $W(H_2)$, embedded in $\mathrm{GL}_n(\mathbb{Z})$ in the natural way, i.e., by their action on the character group of a fixed split maximal torus, have the property that every element of $W(H_1)$ is $\mathrm{GL}_n(\mathbb{Z})$ -conjugate to one in $W(H_2)$, and vice versa, then the Weyl groups are isomorphic.

We prove this result by induction on the rank of the groups H_i . Our proof uses the knowledge of characteristic polynomials of elements in the Weyl groups considered as subgroups of $\mathrm{GL}_n(\mathbb{Z})$.

This study seems relevant for the study of Mumford-Tate groups over algebraic number fields.

0.B. Orders of finite semisimple groups. It is a theorem of Artin ([2, 3]) and Tits ([41, 42, 43, 46, 47, 48]) that if H_1 and H_2 are two finite simple groups of the same order then they are isomorphic except for the pairs

$$(\mathrm{PSL}_4(\mathbb{F}_2), \mathrm{PSL}_3(\mathbb{F}_4)) \text{ and } (\mathrm{PSO}_{2n+1}(\mathbb{F}_q), \mathrm{PSp}_{2n}(\mathbb{F}_q)) \text{ for } n \geq 3, q \text{ odd.}$$

We investigate the situation for the finite semisimple groups in [13]. These are the groups of \mathbb{F}_q -rational points of semisimple algebraic groups defined over the field \mathbb{F}_q .

We concentrate only on the simply connected groups, as the order of $H(\mathbb{F}_q)$ is the same as the order of $H_1(\mathbb{F}_q)$ if H_1 is isogenous to H (Lemma II.10). It is easy to see that the order of $H(\mathbb{F}_q)$ does not determine the group H up to isogeny, for instance

$$|A_1A_3(\mathbb{F}_q)| = |A_2B_2(\mathbb{F}_q)|.$$

However, we prove that the field F_q can be determined under some mild conditions. Since $|A_1(\mathbb{F}_9)| = |B_2(\mathbb{F}_2)|$, the field \mathbb{F}_q can not be determined in general. We feel that this is the only counter example where the field \mathbb{F}_q is not determined by the order of $H(\mathbb{F}_q)$, but we have not been able to prove it. We also observe that for two split, connected, semisimple algebraic groups H_1, H_2 defined over \mathbb{F}_q , $H_i(\mathbb{F}_q)$ have the same order for $i = 1, 2$, then so do the groups $H_i(\mathbb{F}_{q^r})$ for any $r \geq 1$.

The question now boils down to describing the pairs of *order coincidence*, i.e., the pairs of split, semisimple, simply connected \mathbb{F}_q -groups (H_1, H_2) such that the order of the group $H_1(\mathbb{F}_q)$ is the same as the order of the group $H_2(\mathbb{F}_q)$. We want to understand the reason behind the coincidence of these orders and to characterize all possible pairs of order coincidence (H_1, H_2) . We note (Theorem IV.8) that for such a pair (H_1, H_2) , the fundamental degrees of the corresponding Weyl groups, $W(H_1)$ and $W(H_2)$, must be the same with the same multiplicities. Then the following easy observations follow from the basic theory of the Weyl groups ([19]).

Remark (Remark IV.10). *Let H_1 and H_2 be two split semisimple simply connected algebraic groups over a finite field \mathbb{F}_q such that the groups $H_1(\mathbb{F}_q)$ and $H_2(\mathbb{F}_q)$ have the same order. Then we have:*

- (1) *The rank of the group H_1 is the same as the rank of H_2 .*
- (2) *The number of direct simple factors of the groups H_1 and H_2 is the same.*
- (3) *If one of the groups, say H_1 , is simple, then so is H_2 and in that case H_1 is isomorphic to H_2 or $\{H_1, H_2\} = \{B_n, C_n\}$.*

Next natural step would be to look at the pairs of order coincidence in the case of groups each having two simple factors. We characterize such pairs in the theorem (IV.11). There are three infinite families of such pairs,

$$(A_{2n-2}B_n, A_{2n-1}B_{n-1})_{n \geq 2}, (A_{n-2}D_n, A_{n-1}B_{n-1})_{n \geq 4}, (B_{n-1}D_{2n}, B_{2n-1}B_n)_{n \geq 2};$$

and five pairs containing the exceptional group G_2 ,

$$(A_1A_5, A_4G_2), (A_1B_3, B_2G_2), (A_1D_6, B_5G_2), (A_2B_3, A_3G_2) \text{ and } (B_3^2, D_4G_2).$$

Observe that if we define $(H_1, H_2) \circ (H_3, H_4)$ to be the pair obtained by removing the common simple direct factors from the pair (H_1H_3, H_2H_4) , then the above

list is generated by the following pairs:

$$(A_{2n-2}B_n, A_{2n-1}B_{n-1})_{n \geq 2}, \quad (A_{n-2}D_n, A_{n-1}B_{n-1})_{n \geq 4} \quad \text{and} \quad (A_2B_3, A_3G_2).$$

These three pairs admit a geometric reasoning for the order coincidence, we elaborate on it at the end of this subsection.

If we do not restrict ourselves to the groups having exactly two simple factors, then we find the following pairs involving other exceptional groups:

$$(A_1B_4B_6, B_2B_5F_4), \quad (A_4G_2A_8B_6, A_3A_6B_5E_6), \quad (A_1B_7B_9, B_2B_8E_7),$$

$$\text{and} \quad (A_1B_4B_7B_{10}B_{12}B_{15}, B_3B_5B_8B_{11}B_{14}E_8).$$

One now asks a natural question whether these four pairs, together with the above three pairs, generate all possible pairs of order coincidence. Observe that the binary relation \circ , described above, puts the structure of an abelian group on the set of pairs of order coincidence over \mathbb{F}_q ,

$$\{(H_1, H_2) : |H_1(\mathbb{F}_q)| = |H_2(\mathbb{F}_q)|\},$$

where H_1 and H_2 have no common simple direct factor. We prove that (Theorem IV.14) that this group is generated by the following pairs:

$$(A_{2n-2}B_n, A_{2n-1}B_{n-1})_{n \geq 2}, \quad (A_{n-2}D_n, A_{n-1}B_{n-1})_{n \geq 4}, \quad (A_2B_3, A_3G_2),$$

$$(A_1B_4B_6, B_2B_5F_4), \quad (A_4G_2A_8B_6, A_3A_6B_5E_6), \quad (A_1B_7B_9, B_2B_8E_7)$$

$$\text{and} \quad (A_1B_4B_7B_{10}B_{12}B_{15}, B_3B_5B_8B_{11}B_{14}E_8).$$

Now we describe the geometric reasoning for the order coincidence behind the first three pairs in the above list. The groups O_n , U_n and Sp_n act on the spaces \mathbb{R}^n , \mathbb{C}^n and \mathbb{H}^n , respectively, in a natural way. By restricting this action to the corresponding spheres, we get that the groups O_n , U_n and Sp_n act transitively on the spheres S^{n-1} , S^{2n-1} and S^{4n-1} , respectively. By fixing a point in each of the spheres, we get the corresponding stabilizers as $O_{n-1} \subset O_n$, $U_{n-1} \subset U_n$ and $Sp_{n-1} \subset Sp_n$.

By treating the space $\mathbb{C}^n = \mathbb{R}^{2n}$, we see that the groups $U_n \subset O_{2n}$ act transitively on S^{2n-1} . Since S^{2n-1} is connected, the actions of $SU_n \subset U_n$ and $SO_{2n} \subset O_{2n}$ on S^{2n-1} remain transitive. Thus, we get that the action of SO_{2n} is transitive on S^{2n-1} and after restricting to SU_n the action remains transitive. The stabilizer of a point $a \in S^{2n-1}$ in SO_{2n} is SO_{2n-1} and that in SU_n is SU_{n-1} . Then, by a theorem of Onishchik ([30]), we get that the fundamental degrees of the Weyl groups of the compact Lie groups $SO_{2n} \cdot SU_{n-1}$ and $SO_{2n-1} \cdot SU_n$ are the same. Then it is clear that the orders of the finite semisimple groups $D_n A_{n-2}$ and $A_{n-1} B_{n-1}$ are the same over any finite field \mathbb{F}_q .

Similarly, by treating \mathbb{H}^n as \mathbb{C}^{2n} and repeating the above arguments, we get the inclusion of transitive actions $Sp_n \subset SU_{2n}$, acting on the sphere S^{4n-1} , with $Sp_{n-1} \subset SU_{2n-1}$ as the corresponding stabilizers. This gives us the pair of order

coincidence $(A_{2n-1}B_{n-1}, B_nA_{2n-2})$. The pair (A_1B_3, B_2G_2) can be obtained in a similar way by considering the natural action of $G_2 \subset \mathrm{SO}_7$ on S^6 .

It would be interesting to know if the pairs (4) to (7) of theorem (IV.14) involving exceptional groups are also obtained in this geometric way.

0.C. Excellence properties of F_4 . Let G be an algebraic group defined over a field k . We define the anisotropic kernel of G to be the derived group of the centralizer of any maximal split k -torus in G . It is determined up to isomorphism and we denote it by G_{an} .

We say that G is an *excellent group* if for any extension L of k there exists an algebraic group H defined over k such that $H \otimes_k L$ is isomorphic to the anisotropic kernel of the group $G \otimes_k L$.

This notion was introduced by Kersten and Rehmann ([22]) in analogy with the notion of excellence of quadratic forms introduced and studied by Knebusch ([24, 25]). The excellence properties of some groups of classical type have been studied in [20, 22]. It can be seen that a group of type G_2 is excellent over a field k . Since a simple group of type G_2 is either anisotropic or split, therefore the anisotropic kernel of this group over any extension is either the whole group or it is trivial, and hence it is always defined over the base field. We prove in [14] that a group of type F_4 is also excellent over any field of characteristic other than 2 and 3.

Fix a field k of characteristic other than 2 and 3, let G be a group of type F_4 defined over k and let L be an extension of k . It is known that G , a group of type F_4 , defined over a field k can be described as the group of automorphisms of an Albert algebra, \mathcal{A} , defined over k ([17]). If the split rank of the group $G \otimes_k L$ is 0 or 4, then the respective anisotropic kernels, being either the whole group $G \otimes_k L$ or the trivial subgroup, are defined over k . If the group $G \otimes_k L$ has split rank 1, for an extension L/k , then the corresponding Albert algebra over L can be described as the algebra of 3×3 hermitian matrices over an octonion algebra, say \mathfrak{C} , defined over L . We prove that the anisotropic kernel of the group $G \otimes_k L$ is defined in terms of the norm form of the octonion algebra \mathfrak{C} . Since the octonion algebra \mathfrak{C} is defined over k ([32, Theorem 1.8]), it follows that the anisotropic kernel of $G \otimes_k L$ is defined over k . Thus the group G is an excellent group over k .

0.D. General layout of the thesis. A conscious effort is made to make this thesis self-contained and reader-friendly. Almost all basic results about linear algebraic groups and Galois cohomology, that are used in this thesis, are recalled in the first two chapters. Then while using these results we refer to the first two chapters instead of referring to the original papers, which we have anyway referred to in the introductory chapters. For example, Lang's theorem is recalled

in chapter 2 (Theorem II.4) and while using it in the proof of lemma (III.2) we refer to (II.4) instead of [29].

The sections are numbered cumulatively and independent of the chapters whereas the numbering of the results is done according to the chapters. We have notes at the end of the last three chapters. The notes at the end of chapters 3 and 4 merely contain some remarks, but those at the end of chapter 5 contain a proof communicated by an anonymous referee.

Main results proved in this thesis

Theorem 1 (Theorem III.6). Let k be a number field, a local non-archimedean field or a finite field. Let H_1 and H_2 be two split, semisimple linear algebraic groups defined over k sharing the same set of maximal tori up to k -isomorphism. Then the Weyl groups $W(H_1)$ and $W(H_2)$ are isomorphic. Moreover, if we write the Weyl groups $W(H_1)$ and $W(H_2)$ as a direct product of simple Weyl groups,

$$W(H_1) = \prod_{\Lambda_1} W_{1,\alpha}, \quad \text{and} \quad W(H_2) = \prod_{\Lambda_2} W_{2,\beta},$$

then there exists a bijection $i : \Lambda_1 \rightarrow \Lambda_2$ such that $W_{1,\alpha}$ is isomorphic to $W_{2,i(\alpha)}$ for every $\alpha \in \Lambda_1$.

Theorem 2 (Theorem III.7). Let k, H_1, H_2 be as in the above theorem and assume further that the groups H_1 and H_2 are adjoint. Write H_i as a direct product of simple (adjoint) groups,

$$H_1 = \prod_{\Lambda_1} H_{1,\alpha}, \quad \text{and} \quad H_2 = \prod_{\Lambda_2} H_{2,\beta}.$$

There is a bijection $i : \Lambda_1 \rightarrow \Lambda_2$ such that $H_{1,\alpha}$ is isomorphic to $H_{2,i(\alpha)}$, except for the case when $H_{1,\alpha}$ is a simple group of type B_n or C_n , in which case $H_{2,i(\alpha)}$ could be of type C_n or B_n .

Theorem 3 (Theorem IV.6). Let H_1 and H_2 be two split, semisimple, simply connected algebraic groups defined over finite fields \mathbb{F}_{q_1} and \mathbb{F}_{q_2} respectively. Let X denote the set $\{8, 9, 2^r, p\}$ where $2^r + 1$ is a Fermat prime and p is a prime of the type $2^s \pm 1$. Suppose that for $i = 1, 2$, A_1 is not one of the direct factors of H_i whenever $q_i \in X$ and B_2 is not a direct factor of H_i whenever $q_i = 3$. Then, if $|H_1(\mathbb{F}_{q_1})| = |H_2(\mathbb{F}_{q_2})|$, the characteristics of \mathbb{F}_{q_1} and \mathbb{F}_{q_2} are the same.

Theorem 4 (Theorem IV.8). Let H_1 and H_2 be two split, semisimple, simply connected algebraic groups defined over finite fields \mathbb{F}_{q_1} and \mathbb{F}_{q_2} of the same characteristic. Suppose that the order of the finite groups $H_1(\mathbb{F}_{q_1})$ and $H_2(\mathbb{F}_{q_2})$ are the same, then $q_1 = q_2$. Moreover the fundamental degrees (and the multiplicities) of the Weyl groups $W(H_1)$ and $W(H_2)$ are the same.

Theorem 5 (Theorem IV.9). Let H_1 and H_2 be two split, semisimple, simply connected algebraic groups defined over a finite field \mathbb{F}_q . If the orders of the finite groups $H_1(\mathbb{F}_q)$ and $H_2(\mathbb{F}_q)$ are same then the orders of $H_1(\mathbb{F}_{q'})$ and $H_2(\mathbb{F}_{q'})$ are the same for any finite extension $\mathbb{F}_{q'}$ of \mathbb{F}_q .

Theorem 6 (Theorem IV.14). Fix a finite field \mathbb{F}_q and let \mathcal{G} denote the set of pairs (H_1, H_2) of split, semisimple, simply connected algebraic groups defined over \mathbb{F}_q such that H_1, H_2 have no common direct simple factor and $|H_1(\mathbb{F}_q)| = |H_2(\mathbb{F}_q)|$. The set \mathcal{G} admits a structure of an abelian group and it is generated by the following pairs of order coincidences:

- (1) $(A_{2n-2}B_n, A_{2n-1}B_{n-1})$ for $n \geq 2$ with the convention that $B_1 = A_1$,
- (2) $(A_{n-2}D_n, A_{n-1}B_{n-1})$ for $n \geq 4$,
- (3) (A_2B_3, A_3G_2) ,
- (4) $(A_1B_4B_6, B_2B_5F_4)$,
- (5) $(A_4G_2A_8B_6, A_3A_6B_5E_6)$,
- (6) $(A_1B_7B_9, B_2B_8E_7)$,
- (7) $(A_1B_4B_7B_{10}B_{12}B_{15}, B_3B_5B_8B_{11}B_{14}E_8)$.

Theorem 7 (Theorem V.3). Let k be a field of characteristic other than 2 and 3 and let G be a group of type F_4 defined over k . Then for any extension L/k , there exists a linear algebraic group H such that $H \otimes_k L$ is isomorphic to the anisotropic kernel of $G \otimes_k L$.

CHAPTER I

Linear algebraic groups

This chapter is the most basic and at the same time the most essential part of this thesis. Here we define all the required terms and review the basic results that are needed later in this thesis. The theory of linear algebraic groups is a well-developed topic and at least three excellent books are available on it, written by Borel [4], Humphreys [18] and Springer [39]. In addition to these, several expository articles are written by many leading mathematicians working in this area. We refer to them as we use them.

The exposition in this chapter is mostly based on the book by Springer [39]. The first section covers the definition of a linear algebraic group and some very basic properties of linear algebraic groups. In the second section, we introduce the notion of a reductive group. Then in §3, we introduce the notion of a torus to study the reductive groups. The fourth section describes the classification of split simple linear algebraic groups and the last section describes the groups of type G_2 and F_4 .

We fix a perfect field k for this chapter and \bar{k} denotes the algebraic closure of k .

§1. Definition and basic properties.

A *linear algebraic group* G defined over k is a group as well as an affine algebraic variety defined over k such that the maps $\mu : G \times G \rightarrow G$ and $i : G \rightarrow G$, given by $(g_1, g_2) \mapsto g_1 g_2$ and $g \mapsto g^{-1}$, are morphisms of varieties and the identity element, e , is a k -rational point of G .

We sometimes use the word *k -group* to denote a linear algebraic group defined over the field k . If L/k is a field extension and G is a k -group, then the underlying variety of G is also defined over L . The L -group thus obtained is denoted by $G \otimes_k L$.

A *homomorphism of k -groups* $\phi : G \rightarrow H$ is a group homomorphism as well as a morphism of varieties. A surjective homomorphism $\psi : G \rightarrow H$ with a finite kernel is called an *isogeny*. A subgroup H of a linear algebraic group G is assumed to be a closed subset of G (in the Zariski topology). Thus, a subgroup H of a linear algebraic group G is also a linear algebraic group in its own right and the injection $H \hookrightarrow G$ is a homomorphism of algebraic groups.

For k -groups, the notions of connectedness and irreducibility coincide. The maximal irreducible subset in a k -group G containing the identity element is a normal connected subgroup of G of finite index. We call it the connected component of G and denote it by G° .

An example of a linear algebraic group is the group of $n \times n$ invertible matrices, GL_n . Indeed, we have

$$\mathrm{GL}_n = \left\{ \begin{pmatrix} X & 0 \\ 0 & x_{n+1} \end{pmatrix} : \det(X) \cdot x_{n+1} = 1 \right\},$$

and for $X, Y \in \mathrm{GL}_n$, the entries of the product XY are polynomial functions in the entries of X and Y . This group is also known as the *general linear group*.

Observe that there is a difference between GL_n and $\mathrm{GL}_n(k)$. Here, GL_n is an affine algebraic variety defined over k whereas $\mathrm{GL}_n(k)$ is the set of k -rational points of this variety. Similarly, if G is a linear algebraic group defined over k and if L is a field extension of k , then we use the symbol $G(L)$ to denote the set of L -rational points of G .

It is customary to denote the group GL_1 by \mathbb{G}_m . There is another important k -group which is denoted by \mathbb{G}_a for which $\mathbb{G}_a(L) = L$ for every extension L/k . Once we have that GL_n is a k -group, we get plenty of examples of k -groups by looking at the closed subgroups of GL_n . We list some of them below:

- (1) The group of invertible diagonal matrices, D_n , (observe that $D_n \cong \mathbb{G}_m^n$).
- (2) The group of upper triangular matrices, T_n .
- (3) The group of unipotent upper triangular matrices, U_n , (observe that $\mathbb{G}_a \cong U_2$).
- (4) The *special linear group*, $\mathrm{SL}_n = \{X \in \mathrm{GL}_n : \det(X) = 1\}$.
- (5) The *orthogonal group*, $\mathrm{O}_n = \{X \in \mathrm{GL}_n : {}^t X X = 1_n\}$, where ${}^t X$ denotes the transpose of the matrix X and 1_n is the identity matrix in GL_n .
- (6) The *symplectic group*, $\mathrm{Sp}_n = \{X \in \mathrm{GL}_{2n} : {}^t X J X = J\}$, where $J \in \mathrm{GL}_{2n}$ is the matrix $\begin{pmatrix} 0 & 1_n \\ -1_n & 0 \end{pmatrix}$.

In fact, every linear algebraic group is a closed subgroup of GL_n .

(I.1) Theorem ([39, Theorem 2.3.7]). *Let G be a linear algebraic group defined over k . There exists an isomorphism (defined over k) of G onto a closed subgroup of GL_n for some n .*

This theorem implies that no matter what group structure we put on an affine algebraic variety, if it becomes an algebraic group then this group structure can always be seen as multiplication of matrices. It also explains why we use the word *linear* for the affine algebraic groups.

§2. Structural properties of linear algebraic groups.

Now that a linear algebraic group is a matrix group, we can use all the linear algebraic tools like eigenvalues, diagonalization and semisimplicity to study the linear algebraic groups. Recall that a matrix in $\mathrm{GL}_n(k)$ is called *semisimple* (respectively, *unipotent*) if it is diagonalizable over the algebraic closure of k (respectively, if all its eigenvalues are equal to 1). Recall also that a matrix $X \in \mathrm{GL}_n(k)$ can be written as $X = X_s X_u = X_u X_s$ in a unique way, where $X_s \in \mathrm{GL}_n(k)$ is a semisimple matrix and $X_u \in \mathrm{GL}_n(k)$ is a unipotent matrix. This is called the Jordan decomposition of matrices. We have the following analog of the Jordan decomposition in linear algebraic groups.

(I.2) Theorem ([39, Theorem 2.4.8]). *Let G be a linear algebraic group defined over k and let $g \in G$.*

- (1) *There exist unique elements $g_s, g_u \in G$ such that $g = g_s g_u = g_u g_s$, where the image of g_s (respectively, the image of g_u) under any injection $\rho : G \hookrightarrow \mathrm{GL}_n$ is a semisimple (respectively, a unipotent) matrix.*
- (2) *If $\phi : G \rightarrow G'$ is a homomorphism of linear algebraic groups, then $\phi(g_s) = \phi(g)_s$ and $\phi(g_u) = \phi(g)_u$.*

The elements g_s and g_u in (1) are called the *semisimple part* and the *unipotent part* of $g \in G$ respectively. We call an element $g \in G$ to be *semisimple* (respectively, *unipotent*) if $g = g_s$ (respectively, if $g = g_u$).

A k -group G is said to be *unipotent* if all its elements are unipotent. It can be shown that a unipotent k -group is always isomorphic (over k) to some (closed) subgroup of U_n . For a k -group G , (G, G) denotes the subgroup of G generated by all elements of the type $g_1 g_2 g_1^{-1} g_2^{-1}$. If the group G is connected, then (G, G) is a closed subgroup of G and is called the *derived group* of G . We say that a k -group G is *solvable* if it is so as an abstract group.

The *radical* of a k -group G is defined to be the maximal closed, connected, normal, solvable k -subgroup of G . It exists and is denoted by $R(G)$. Similarly the maximal closed, connected, normal, unipotent k -subgroup of G is called the *unipotent radical* of G and we denote it by $R_u(G)$. Clearly, $R_u(G)$ is a subgroup of $R(G)$. Moreover, $R_u(G)$ is precisely the subset consisting of all unipotent elements in $R(G)$.

A linear algebraic group G defined over the field k , is called *reductive* if the unipotent radical of G is trivial. If the radical of G is trivial, then we call G to be a *semisimple algebraic group*. If a k -group G has no connected, closed, normal k -subgroup then we say that G is a *simple algebraic group*.

As an example, we see that the group $\mathrm{GL}_n \times \mathrm{GL}_m$ is reductive, the group $\mathrm{SL}_n \times \mathrm{SL}_m$ is semisimple and the group SL_n is a simple algebraic group. A simple

algebraic group is always semisimple and a semisimple algebraic group is always a reductive group.

A reductive k -group G can be decomposed as an almost direct decomposition, i.e., a decomposition where the components are allowed to have finite intersections, of simple k -groups and the radical of G .

(I.3) Theorem ([39, Theorem 8.1.5 and Corollary 8.1.6]). *If G is a connected reductive algebraic group defined over k , then we can write G as an almost direct decomposition*

$$G = G_1 \cdots G_r \cdot R(G),$$

where G_i are simple algebraic groups defined over k and $R(G)$ is the radical of the group G .

We call the simple groups G_i that appear in the above decomposition of G the *simple direct factors* of the group G . From the above theorem, it is clear that we have to understand the structure of simple k -groups to understand the structure of reductive k -groups. It turns out that the simple k -groups can be classified explicitly up to (central) isogeny. A *central isogeny* is an isogeny $\phi : G \rightarrow H$ whose (finite) kernel is contained in the center of G .

A connected k -group G is said to be *simply connected* if, for any connected group H , any central isogeny $\phi : H \rightarrow G$ is an isomorphism. A connected k -group G is said to be *adjoint* if, for any connected group H , any central isogeny $\phi : G \rightarrow H$ is an isomorphism. The simply connected and adjoint groups are sort of end objects for semisimple algebraic groups, as the following theorem suggests.

(I.4) Theorem ([34, Proposition 2.10]).

- (1) *Let G be a semisimple k -group. There exist a simply connected group \tilde{G} , an adjoint group \overline{G} and central isogenies*

$$\tilde{G} \xrightarrow{\pi} G \xrightarrow{\phi} \overline{G}.$$

- (2) *Any simply connected (respectively, adjoint) semisimple k -group is a direct product of simple k -groups which, moreover, are simply connected (respectively, adjoint).*

§3. Tori in reductive groups.

We introduce the notion of a torus to study the semisimple elements. Throughout this section, G denotes a reductive k -group.

A *torus* (or a *k -torus*) is a k -group which is \bar{k} -isomorphic to \mathbb{G}_m^n for some n . If a k -torus T is k -isomorphic to some \mathbb{G}_m^n , then we say that it is a *k -split torus*

or simply a *split torus* if there is no confusion about the base field. Note that a k -torus need not be k -split. For instance,

$$T = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \in \mathrm{GL}_2 : a^2 + b^2 = 1 \right\}$$

is a torus defined over \mathbb{Q} , but it is not split over \mathbb{Q} .

3.A. Maximal tori. A torus in G is called *maximal* if it is not properly contained in any other torus in G . Such tori exist because of the dimension argument. It is clear that all elements in a k -torus are semisimple. Moreover, every semisimple element $g \in G(k)$ is contained in some maximal k -torus in G and, in fact, any k -torus in G is contained in some maximal k -torus in G .

As we have seen above, a maximal torus in G need not be split over k . However, there may be tori in G which are maximal with respect to being split over k . We call such tori *maximal k -split* tori in G . If T_1 and T_2 are two maximal k -split tori in G then there exists an element $g \in G(k)$ such that $T_1 = gT_2g^{-1}$ ([34, 2.1.14]). Hence the dimension of a maximal k -split torus is independent of any fixed maximal k -split torus and we call it the *k -rank* of the group G or the *split rank of G over k* .

Since any k -torus is split over \bar{k} , we have that any two maximal k -tori in G can be conjugated by an element of $G(\bar{k})$. The \bar{k} -rank of G is called simply the *rank* of the group G . If the \bar{k} -rank of G is the same as its k -rank, in other words, if the group G has a maximal k -torus which is split over k , then G is said to be a *split reductive k -group*. We call G to be *isotropic* if it contains a (not necessarily maximal) k -split torus and it is called *anisotropic* if it contains no split torus.

3.B. Weyl group. The maximal tori in G are special in the sense that the connected component of the centralizer of a maximal torus in the group G is the torus itself, i.e., $Z_G(T)^\circ = T$ for a maximal torus T in G . Moreover, the torus T is a finite index normal subgroup of its normalizer in G , $N_G(T)$. The finite quotient $N_G(T)/T$ is defined to be the *Weyl group of G* with respect to the torus T and it is denoted by $W(G, T)$. If the group G is split over k , then we can choose T to be a split maximal torus and we denote the corresponding Weyl group by $W(G)$.

If we decompose the reductive k -group G as an almost direct decomposition of simple k -groups and the radical of G , say, $G = G_1 \cdots G_r \cdot R(G)$, then the Weyl group of G is a direct product of the Weyl groups of simple direct factors of G ,

$$W(G) = W(G_1) \cdots W(G_r).$$

If there is a central isogeny $\phi : G \rightarrow H$, then the Weyl group of H is isomorphic to the Weyl group of G .

3.C. Anisotropic kernel. The split semisimple k -groups are well understood. They are determined, up to an isogeny, by their direct simple factors. It is desirable to determine the isotropic groups and the anisotropic ones by some data. We now introduce the notion of anisotropic kernel which helps us in understanding the structure of isotropic groups. This notion is motivated by the notion of the anisotropic kernel in the theory of quadratic forms.

Let S be a maximal k -split torus in G . The derived group of $Z_G(S)$, the centralizer of the torus S in G , is called the *anisotropic kernel* of the group G with respect to the torus S ([44, §2]). Since any two maximal k -split tori, say S_1 and S_2 , are conjugate over k , the anisotropic kernels of G with respect to S_i are k -isomorphic. Hence the anisotropic kernel is determined up to k -isomorphism and we denote it by G_{an} .

It is clear that if G is anisotropic then $G_{an} = (G, G)$ whereas in the other extreme if G is k -split then G_{an} is trivial. The general theory of isotropic and anisotropic groups does not appear in this thesis until the last chapter.

§4. Classification of simple algebraic groups.

The split simple k -groups are easier to handle than the general simple k -groups, therefore we first classify the split simple algebraic groups defined over the field k . For that, we introduce the notion of a root system. The root system can be defined in an axiomatic way, but we avoid doing it here. Instead, we compute the root system of a split semisimple k -group explicitly.

4.A. Root system. Let G be a split semisimple k -group and fix a split maximal k -torus T in G . A *character* of the torus T is a homomorphism (of k -groups) $\chi : T \rightarrow \mathbb{G}_m$ and a *cocharacter* of T is a homomorphism $\lambda : \mathbb{G}_m \rightarrow T$. The characters as well as cocharacters admit the natural structure of a free abelian group and we denote them respectively by $X^*(T)$ and $X_*(T)$. Thus,

$$X^*(T) := \{\chi : T \rightarrow \mathbb{G}_m\}, \quad X_*(T) := \{\lambda : \mathbb{G}_m \rightarrow T\}.$$

For $\chi \in X^*(T)$ and $\lambda \in X_*(T)$, we define the character of \mathbb{G}_m given by $a \mapsto \chi(\lambda(a))$. Hence there is an integer, which we denote by $\langle \chi, \lambda \rangle$, such that $\chi(\lambda(a)) = a^{\langle \chi, \lambda \rangle}$. We thus have a bilinear map $\langle \cdot, \cdot \rangle : X^*(T) \times X_*(T) \rightarrow \mathbb{Z}$.

The group G acts on its Lie algebra by the adjoint action. We can then decompose the Lie algebra into T -invariant subspaces corresponding to the characters of T . The nonzero characters that correspond to the non-trivial T -invariant subspaces are called *roots* of G with respect to T . We denote the set of all roots of G with respect to T by $\Phi(G, T)$.

Since the group G is k -split, it can be shown that $X^*(T)$, $X_*(T)$ and $\Phi(G, T)$ are independent of the chosen split maximal torus T , so we denote them respectively by $X(G)$, $X^\vee(G)$ and $\Phi(G)$ (or simply by X , X^\vee and Φ). The set Φ

generates the group X . Define $V := \mathbb{R} \otimes X$. It is clear that the finite set Φ generates V over \mathbb{R} and we call it a *root system* in V . An isomorphism between two root systems Φ_i in V_i , for $i = 1, 2$, is an isomorphism of vector spaces $\phi : V_1 \rightarrow V_2$ such that $\phi(\Phi_1) = \Phi_2$.

There exists a basis of X in Φ , denoted by Π , such that any element in Φ is a linear combination of elements of Π with all coefficients of the same sign. The elements of Π are called as *simple roots*. For each $\alpha \in \Phi$, we can choose an element $\alpha^\vee \in X^\vee$ in a canonical way such that $\langle \alpha, \alpha^\vee \rangle = 2$. We denote the set of all α^\vee by Φ^\vee .

It can be shown that the root system Φ is reduced, i.e., if $\alpha, c\alpha \in \Phi$ for $c \in \mathbb{R}^\times$, then $c = \pm 1$. For any two linearly independent roots $\alpha, \beta \in \Phi$, we have that $\langle \alpha, \beta^\vee \rangle$ is 0, ± 1 , ± 2 or ± 3 and $0 < \langle \alpha, \beta^\vee \rangle \langle \beta, \alpha^\vee \rangle \leq 3$.

We now define the *Dynkin diagram* of the group G , denoted by $D(G)$, to be the graph whose vertex set is $\Pi(G)$, the set of simple roots of G , and two vertices $\alpha, \beta \in \Pi(G)$ are joined by $\langle \alpha, \beta^\vee \rangle \langle \beta, \alpha^\vee \rangle$ edges, with an arrow pointing towards the shorter root if α and β have different lengths.

We call a root system to be *reducible* if it can be obtained by taking direct sum of two root systems and *irreducible* otherwise. The Dynkin diagram of an irreducible root system is a connected graph and it does not contain a circuit (though it can have multiple edges). The irreducible root systems can be explicitly classified and they exactly correspond to the split simple k -groups.

(I.5) Theorem ([39, §9.6]). *A connected, split, semisimple k -group G is determined up to central isogeny by the isomorphism class of its root system, $\Phi(G)$.*

(I.6) Theorem ([28, Proposition 25.8]). *Let G be a connected, split semisimple k -group.*

- (1) *The group G is simple if and only if the root system $\Phi(G)$ is irreducible if and only if the Dynkin diagram $D(G)$ is connected.*
- (2) *If G_i are the simple direct factors of the group G , then $\Phi(G) \xrightarrow{\sim} \bigoplus_i \Phi(G_i)$ and the Dynkin diagram of G , $D(G)$, is the disjoint union of $D(G_i)$.*

We now list the split simple k -groups. There are four infinite families of split simple k -groups, which are also called classical simple groups, A_n , B_n , C_n and D_n . In addition to these, there are five exceptional groups, G_2 , F_4 , E_6 , E_7 and E_8 .

4.B. Classical split simple k -groups. We first describe the classical split simple k -groups. For each such group G , we describe the root system $\Phi(G)$, simple roots $\Pi(G)$ and the Weyl group $W(G)$.

4.B.1. Type A_n , ($n \geq 1$). This is the first infinite family of classical split simple groups. It corresponds to the special linear groups SL_{n+1} described in §1. The group SL_{n+1} is simply connected whereas the corresponding adjoint group is denoted by PSL_{n+1} .

We now describe the root system of SL_{n+1} . Let $V_1 = \mathbb{R}^{n+1}$ and let V be the quotient vector space of V_1 by the 1-dimensional subspace generated by the vector $e_1 + e_2 + \cdots + e_{n+1}$ where $\{e_1, \dots, e_{n+1}\}$ is the canonical basis of V_1 . We denote by \bar{e}_i the class of e_i in V . The roots and simple roots of SL_{n+1} are given by:

$$\{\bar{e}_i - \bar{e}_j : i \neq j\},$$

$$\{\alpha_1 = \bar{e}_1 - \bar{e}_2, \dots, \alpha_n = \bar{e}_n - \bar{e}_{n+1}\},$$

and the Dynkin diagram of SL_{n+1} is given by: $\begin{array}{ccccccc} \circ & \text{---} & \circ & \text{---} & \cdots & \text{---} & \circ \\ \alpha_1 & & \alpha_2 & & & & \alpha_n \end{array}$.

The Weyl group of SL_{n+1} is S_{n+1} , the symmetric group acting on $n+1$ symbols.

4.B.2. Type B_n , ($n \geq 2$). This family of split simple k -groups corresponds to the special orthogonal groups $\mathrm{SO}_{2n+1} = \mathrm{SL}_{2n+1} \cap \mathrm{O}_{2n+1}$. This group is adjoint and the corresponding simply connected group is denoted by Spin_{2n+1} .

The root system for B_n is given as follows. Let $V = \mathbb{R}^n$ with canonical basis $\{e_i\}$. Then the set of roots and the set of simple roots of SO_{2n+1} are given by:

$$\{\pm e_i, \pm e_i \pm e_j : i \neq j\},$$

$$\{\alpha_1 = e_1 - e_2, \dots, \alpha_{n-1} = e_{n-1} - e_n, \alpha_n = e_n\},$$

and the corresponding Dynkin diagram is $\begin{array}{ccccccc} \circ & \text{---} & \circ & \text{---} & \cdots & \text{---} & \circ \rightleftarrows \circ \\ \alpha_1 & & \alpha_2 & & & & \alpha_{n-1} \quad \alpha_n \end{array}$.

The Weyl group of SO_{2n+1} is isomorphic to $S_n \ltimes (\mathbb{Z}/2\mathbb{Z})^n$. The semidirect product is given by the natural permutation action of S_n on $(\mathbb{Z}/2\mathbb{Z})^n$.

4.B.3. Type C_n , ($n \geq 3$). This family of classical split simple k -groups corresponds to the symplectic groups Sp_n , as described in §1. The group Sp_n is simply connected and the corresponding adjoint group is denoted by PGSp_n .

Let $V = \mathbb{R}^n$ with the canonical basis $\{e_i\}$. Then the root system and the set of simple roots of Sp_n are given by:

$$\{\pm 2e_i, \pm e_i \pm e_j : i \neq j\},$$

$$\{\alpha_1 = e_1 - e_2, \dots, \alpha_{n-1} = e_{n-1} - e_n, \alpha_n = 2e_n\},$$

and the corresponding Dynkin diagram is $\begin{array}{ccccccc} \circ & \text{---} & \circ & \text{---} & \cdots & \text{---} & \circ \leftleftarrows \circ \\ \alpha_1 & & \alpha_2 & & & & \alpha_{n-1} \quad \alpha_n \end{array}$.

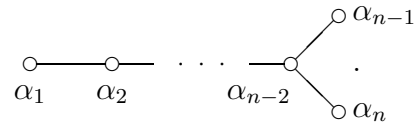
The Weyl group of Sp_n is the same as $W(B_n)$, $S_n \ltimes (\mathbb{Z}/2\mathbb{Z})^n$.

4.B.4. Type D_n , ($n \geq 4$). This family of split simple k -groups corresponds to the special orthogonal groups $\mathrm{SO}_{2n} = \mathrm{SL}_{2n} \cap \mathrm{O}_{2n}$. The corresponding simply connected and adjoint groups are denoted respectively by Spin_{2n} and PGSO_{2n} .

Let $V = \mathbb{R}^n$ with canonical basis $\{e_i\}$. Then the root system and the set of simple roots of SO_{2n} are given by:

$$\{\pm e_i \pm e_j : i \neq j\},$$

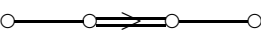
$$\{\alpha_1 = e_1 - e_2, \dots, \alpha_{n-1} = e_{n-1} - e_n, \alpha_n = e_{n-1} + e_n\},$$

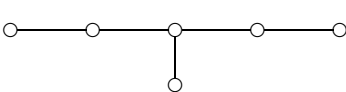
and the corresponding Dynkin diagram is 

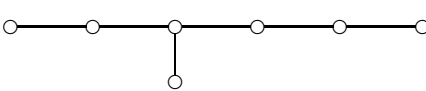
The Weyl group of SO_{2n} is isomorphic to $S_n \ltimes (\mathbb{Z}/2\mathbb{Z})^{n-1}$. This is the subgroup of $S_n \ltimes (\mathbb{Z}/2\mathbb{Z})^n$ consisting of elements $(\sigma, (x_1, \dots, x_n))$, $\sigma \in S_n, x_i \in \mathbb{Z}/2\mathbb{Z}$, such that $\sum_i x_i = 0$.

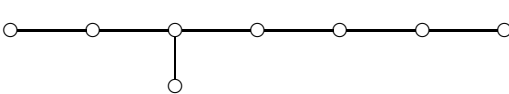
4.C. Exceptional split simple k -groups. We now come to the five exceptional types of split simple k -groups. These groups are not as easy as the classical groups to handle. The models of these types are described by the non-associative algebras. We study the octonion algebras and the Albert algebras in the next section and describe the groups of type G_2 and F_4 . We are not going to say anything else for other three types, namely E_6, E_7 and E_8 . For now, we just give the Dynkin diagrams for these five exceptional split simple k -groups.

G_2 : 

F_4 : 

E_6 : 

E_7 : 

E_8 : 

We summarise the information about the split simple k -groups in the following table.

Table 1

Type of G	order of $\Phi(G)$	order of $\Pi(G)$ = rank of G	order of $W(G)$
A_n	$n(n+1)$	n	$(n+1)!$
B_n	$2n^2$	n	$2^n \cdot n!$
C_n	$2n^2$	n	$2^n \cdot n!$
D_n	$2n(n-1)$	n	$2^{n-1} \cdot n!$
G_2	12	2	12
F_4	48	4	$2^7 \cdot 3^2$
E_6	72	6	$2^7 \cdot 3^4 \cdot 5$
E_7	126	7	$2^{10} \cdot 3^4 \cdot 5 \cdot 7$
E_8	240	8	$2^{14} \cdot 3^5 \cdot 5^2 \cdot 7$

4.D. Non-split simple k -groups. Observe that any simple k -group is split by a finite Galois extension of k . Further, we observe that the list of the split simple k -groups does not depend on the field k . That is to say that the list is the same for any two fields. Therefore, if we consider an extension L/k and suppose that G is a split simple L -group, then we can find a split simple k -group H such that $H \otimes_k L$ is L -isogenous to G . This group H can be taken to be the k -group corresponding to the root system of G . So the question now boils down to describe the simple k -groups which are isomorphic to a fixed split simple k -group over some extension L/k . This is done using Galois cohomology and we describe it in the next chapter.

§5. Groups of type G_2 and F_4 .

We first review the theory of octonion algebras and the Albert algebras. An excellent reference for this is the book by Springer and Veldkamp [40]. For simplicity, we assume in this section that the characteristic of the field k is other than 2 and 3.

5.A. Octonion algebras and groups of type G_2 . A *composition algebra* C over k is a finite dimensional (not necessarily associative) k -algebra with identity element together with a non-degenerate quadratic form N , called the *norm form*, such that

$$N(x)N(y) = N(xy) \quad \forall x, y \in C.$$

It turns out that the possibilities for the dimensions of a composition algebra over k are 1, 2, 4 or 8. A composition algebra comes equipped with an involution $\bar{} : C \rightarrow C$ such that $x\bar{x} = \bar{x}x = N(x)$. The norm form of a composition algebra is a Pfister form, therefore it is either anisotropic, i.e., it has no nontrivial zero, or it achieves the maximum possible Witt index.

An *octonion algebra* over k is a composition algebra over k of dimension 8. It is a non-associative algebra. An octonion algebra is said to be *split* (respectively, *anisotropic*) if its norm form is isotropic (respectively, anisotropic). An octonion algebra is determined by its norm form, hence there is a unique split octonion algebra over k . We now describe the split octonion algebra over k .

Let \mathbb{M}_2 denote the 2×2 matrix algebra and define $\mathfrak{C} = \mathbb{M}_2 \oplus \mathbb{M}_2$. For $x \in \mathbb{M}_2$, let \bar{x} be the adjoint matrix of x , i.e.,

$$\overline{\begin{pmatrix} a & b \\ c & d \end{pmatrix}} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

We now define the multiplication in \mathfrak{C} and the norm form over \mathfrak{C} as

$$(x, y)(u, v) = (xu + \bar{v}y, vx + y\bar{u}) \quad \text{and} \quad N((x, y)) = \det(x) - \det(y).$$

It can be easily checked that the form N is a non-degenerate quadratic form and that it is multiplicative on \mathfrak{C} . Thus, \mathfrak{C} is an octonion algebra. Further, the norm form N clearly has non-trivial zeros, therefore the octonion algebra \mathfrak{C} is split.

The octonion algebras over the field k describe the k -groups of type G_2 .

(I.7) Theorem (Hijikata [17, page 163]). *Let G be a simple algebraic group of type G_2 defined over the field k . Then there exists an octonion algebra \mathfrak{C} , unique upto isomorphism, defined over k such that G is k -isomorphic to the group of k -automorphisms of \mathfrak{C} , $\text{Aut}_k(\mathfrak{C})$.*

5.B. Albert algebras and groups of type F_4 . Let \mathfrak{C} denote an octonion algebra over the field k and let N denote the norm form of \mathfrak{C} . Consider $\mathbb{M}_3(\mathfrak{C})$, the (non-associative) algebra of 3×3 matrices with entries from \mathfrak{C} . Let $\Gamma \in \mathbb{M}_3(k)$ be the diagonal matrix with $\gamma_1, \gamma_2, \gamma_3$ on the diagonal. Consider the involution of $\mathbb{M}_3(\mathfrak{C})$ given by $X \mapsto X^* = \Gamma^{-1}({}^t\bar{X})\Gamma$, where \bar{X} is the matrix $\{\bar{X}_{i,j}\}$. We define $\mathcal{H}(\mathfrak{C}; \gamma_1, \gamma_2, \gamma_3)$, which is also denoted by $\mathcal{H}(\mathfrak{C}; \Gamma)$, to be the subset of $\mathbb{M}_3(\mathfrak{C})$ consisting of the fixed points of the involution $X \mapsto X^*$. We have

$$\mathcal{H}(\mathfrak{C}; \Gamma) := \left\{ \begin{pmatrix} x_1 & c_3 & \gamma_1^{-1}\gamma_3\bar{c}_2 \\ \gamma_2^{-1}\gamma_1\bar{c}_3 & x_2 & c_1 \\ c_2 & \gamma_3^{-1}\gamma_2\bar{c}_1 & x_3 \end{pmatrix} : x_i \in k, c_i \in \mathfrak{C} \right\}.$$

This is a 27 dimensional vector space over k . We define the multiplication on $\mathcal{H}(\mathfrak{C}; \Gamma)$ by

$$X \times Y = \frac{1}{2}(XY + YX).$$

This multiplication makes $\mathcal{H}(\mathfrak{C}; \Gamma)$ into a non-associative k -algebra. We also have a quadratic form on it defined by

$$\begin{aligned} Q(X) &= \frac{1}{2} \operatorname{tr}(X^2) \\ &= \frac{1}{2}(x_1^2 + x_2^2 + x_3^2) + \gamma_2 \gamma_3^{-1} N(c_1) + \gamma_3 \gamma_1^{-1} N(c_2) + \gamma_1 \gamma_2^{-1} N(c_3). \end{aligned}$$

We define the *split Albert algebra* over k to be the algebra $\mathcal{H}(\mathfrak{C}; \Gamma)$ where \mathfrak{C} is the split octonion algebra over k . An *Albert algebra* over k is a (non-associative) algebra \mathcal{A}/k such that $\mathcal{A} \otimes_k L$ is isomorphic to the split Albert algebra over L for some extension L/k . A split Albert algebra over k is unique up to isomorphism.

Albert algebras over the field k describe the k -groups of type F_4 .

(I.8) Theorem (Hijikata [17, page 164]). *Let G be a simple algebraic group of type F_4 defined over the field k . Then there exists an Albert algebra \mathcal{A} , unique upto isomorphism, defined over k such that G is k -isomorphic to the group of k -automorphisms of \mathcal{A} , $\operatorname{Aut}_k(\mathcal{A})$.*

CHAPTER II

Galois Cohomology

This is another basic chapter of this thesis. In this chapter, we mainly deal with the Galois cohomology of linear algebraic groups. There are several excellent references for this topic, Platonov-Rapinchuk [34, §2.2 and Ch. 6], Serre [36] and the expository article by Springer [37], to mention a few.

In §6, we define the Galois cohomology sets H^0 and H^1 . The next section deals with the classification of k -forms using Galois cohomology. We also give the results regarding $H^1(k, G)$ for some special fields k . Then in §8, we use Galois cohomology to describe the k -isomorphism classes of k -tori and the conjugacy classes of maximal tori in a split reductive k -group. The last section is in a different direction. We introduce the Herbrand quotient there and prove that the order of a finite semisimple group is an invariant of its isogeny class.

§6. Basic definitions.

Galois cohomology is basically the cohomology of the Galois groups. Let G be a group and let A be an abelian group admitting an action of G such that $g(ab) = g(a)g(b)$ for all $g \in G, a, b \in A$. The group A can be treated as a module over $\mathbb{Z}[G]$ in the natural way, so we also call A to be a G -module. We define A^G to be the largest subgroup of A on which G acts trivially. The cohomology groups, denoted by $H^i(G, A)$ for $i \geq 0$, are the right derived functors of the left exact functor $A \mapsto A^G$ from the category of G -modules to the category of abelian groups. The cohomology groups $H^i(G, A)$ can be computed using the standard cochain complex ([11]). We are interested in the first two cohomology groups, $H^0(G, A)$ and $H^1(G, A)$, and we define them as follows:

$$H^0(G, A) = A^G := \{a \in A : g(a) = a \ \forall g \in G\},$$

$$H^1(G, A) := \frac{\{\phi : G \rightarrow A : \phi(g_1 g_2) = \phi(g_1) g_1(\phi(g_2))\}}{\{\phi_a(g) = a^{-1} g(a) : a \in A\}}.$$

If the group A is not abelian, then usually only H^0 and H^1 are defined. The group $H^0(G, A)$ is again defined to be A^G whereas $H^1(G, A)$ is defined to be the set of equivalence classes of the set

$$Z^1(G, A) := \{\phi : G \rightarrow A : \phi(g_1 g_2) = \phi(g_1) g_1(\phi(g_2))\},$$

where $\phi_1 \sim \phi_2$ if there exists $a \in A$ such that $\phi_1(g) = a^{-1}\phi_2(g)g(a)$ for all $g \in G$. An element of $Z^1(G, A)$ is called a 1-*cocycle*. The set $H^1(G, A)$ is a *pointed set*, i.e., it has a distinguished element called the *neutral element*, namely, the equivalence class of the trivial map $g \mapsto 1$. If A is abelian then these definitions of H^0 and H^1 agree with the above definitions. Observe that if the group G acts trivially on A , then the set $Z^1(G, A)$ is the set of all homomorphisms from G to A . If

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$$

is an exact sequence of groups admitting G -action, then

$$\begin{aligned} 0 \longrightarrow H^0(G, A) \longrightarrow H^0(G, B) \longrightarrow H^0(G, C) \\ \longrightarrow H^1(G, A) \longrightarrow H^1(G, B) \longrightarrow H^1(G, C) \end{aligned}$$

is an exact sequence of pointed sets, i.e., the inverse image of the neutral element under any map is the image of the previous map.

Let k be a field and let K/k be a finite Galois extension. If G is an algebraic group defined over the field k , then the Galois group $\text{Gal}(K/k)$ acts naturally on $G(K)$, the group of K -rational points of G . It is customary to denote $H^i(\text{Gal}(K/k), G(K))$ by $H^i(K/k, G)$. We define

$$H^i(k, G) := \varinjlim H^i(K/k, G),$$

the direct limit taken over all finite Galois extensions of k . Let us see some examples now.

- (1) $H^0(k, G) = G(k)$. In particular, $H^0(k, \mathbb{G}_m) = k^\times$ and $H^0(k, \mathbb{G}_a) = k$.
- (2) $H^1(k, \mathbb{G}_m) = 0$, the Hilbert's theorem 90.
- (3) $H^1(k, \text{GL}_n) = 0$.
- (4) $H^i(k, \mathbb{G}_a) = 0$ for all $i \geq 1$, the normal basis theorem.

§7. Galois cohomology of linear algebraic groups.

In this section, we recall some basic results about the Galois cohomology of linear algebraic groups.

7.A. Classification of k -forms. Fix a field k and let G be a linear algebraic group defined over k . A *principal homogeneous space* of G over k is an algebraic variety P , defined over k , which admits a simple transitive G -action, i.e., there is a morphism of algebraic varieties $\phi : G \times P \rightarrow P$ such that the map

$$(\phi, \pi_2) : G \times P \rightarrow P \times P, \quad (g, p) \mapsto (gp, p)$$

is an isomorphism of varieties. An example of a principal homogeneous space of G is $P = G$ and the map $\phi : G \times G \rightarrow G$ is the multiplication in G . Two principal homogeneous spaces P_1, P_2 of G over k are said to be isomorphic if they are isomorphic under a map which is compatible with the G -action. It is clear

that a principal homogeneous space of G over k is k -isomorphic to G if and only if $P(k) \neq \emptyset$. The following theorem gives a way to describe the set of k -isomorphism classes of the principal homogeneous spaces of G over k .

(II.1) Theorem ([36, §I.5.2]). *Let k be a field and let G be a linear algebraic group defined over k . The set of k -isomorphism classes of principal homogeneous spaces of G over k is in bijection with the set $H^1(k, G)$.*

Now we come to the classification of k -forms of a k -group, which was promised in the first chapter. We state the result in a general form.

Let X be an “algebraic object” defined over the field k . Here an algebraic object could mean a linear algebraic group, an algebraic variety, a division algebra or more generally an associative or a non-associative algebra defined over k . A k -form of X is another algebraic object Y , of the same type as that of X , defined over k which is isomorphic to X over k_s , the separable closure of k . The following theorem gives us a description of k -forms of X .

(II.2) Theorem ([36, §III.1.3]). *Let k, X be as above and let $A := \text{Aut}_k(X)$ denote the group of algebraic k -automorphisms of X . Then $H^1(k, A)$ is in bijection with the set of k -isomorphism classes of the k -forms of X .*

As a corollary, we have:

(II.3) Corollary. *Let k be a field.*

- (1) *For a k -group G , the set of k -isomorphism classes of k -groups H which are k_s -isomorphic to G is in bijection with the set $H^1(k, \text{Aut}_k(G))$.*
- (2) *Let X be one of the split simple k -groups described in §4, then the simple k -groups which are k_s -isomorphic to X can be described by the set $H^1(k, \text{Aut}_k(X))$.*

(These groups are called the simple k -groups of type X .)

It should be pointed out that the above theorem gives only an interpretation of the k -forms of X . It is usually not easy to calculate $H^1(k, \text{Aut}_k(X))$. However, this rephrasing does help in seeing the k -forms in a new perspective. We illustrate this by means of an example.

The group $\text{Aut}_k(\text{SL}_2)$ is isomorphic to PGL_2 which also happens to be the group of k -automorphisms of \mathbb{M}_2 as a central simple algebra over k . Hence $H^1(k, \text{PGL}_2)$ on one hand describes the k -forms of SL_2 and on the other hand it describes the k -forms of \mathbb{M}_2 , i.e., the quaternion algebras defined over k . Thus, one deduces that there is a bijective correspondence between the quaternion algebras over k and the k -forms of SL_2 . Indeed, there is one such correspondence sending a quaternion algebra H to the group of norm 1 elements in H , which is a group of type SL_2 .

7.B. $H^1(k, G)$ for some special fields k . As we saw in (§7.A), the set $H^1(k, G)$ is important by several aspects. Here we give the results concerning the computations of $H^1(k, G)$ over some special ground fields k and for some special types of groups G defined over them. The first such theorem that comes to mind is the following fundamental theorem proved by Lang in 1958.

(II.4) Theorem (Lang [29, Corollary to Theorem 1]). *Let k be a finite field and let G be a connected algebraic group defined over k . Then $H^1(k, G) = 0$.*

Observe that in the above theorem, the group G need not be linear. We have following weaker version of the above theorem for linear algebraic groups defined over local fields.

(II.5) Theorem (Kneser [26, 27], Bruhat-Tits [7, 8, 9, 10]). *Let k be a local field of characteristic 0 and let G be a connected, semisimple, simply connected, linear algebraic group defined over k . Then $H^1(k, G) = 0$.*

§8. Galois cohomology and tori.

Fix a field k and let $T_0 = \mathbb{G}_m^n$ be the split n -dimensional torus defined over k . The special version of the theorem (II.2), where we replace the algebraic object X by the k -torus T_0 , is given by:

(II.6) Lemma. *Let k be a field. The k -isomorphism classes of n -dimensional tori defined over k are in bijection with the isomorphism classes of n -dimensional integral representations of the Galois group $\text{Gal}(\bar{k}/k)$.*

Proof: Let T_1 be an n -dimensional torus defined over k and let L_1 denote a splitting field of T_1 . We assume that the field L_1 is Galois over k . Since the torus T_1 is split over L_1 , we have an L_1 -isomorphism $f : T_0 \rightarrow T_1$. The Galois action on T_0 and T_1 gives us another isomorphism, $f^\sigma := \sigma f \sigma^{-1} : T_0 \rightarrow T_1$ for $\sigma \in \text{Gal}(L_1/k)$. One checks that the map $\sigma \mapsto f^{-1} f^\sigma$ is a 1-cocycle. Indeed,

$$f^{-1} f^{\sigma\tau} = (f^{-1} \sigma f \sigma^{-1}) \sigma (f^{-1} \tau f \tau^{-1}) \sigma^{-1} = (f^{-1} f^\sigma) (f^{-1} f^\tau)^\sigma.$$

By composing the natural map from $\text{Gal}(\bar{k}/k)$ to $\text{Gal}(L_1/k)$ with this map we get a 1-cocycle $\varphi_f : \text{Gal}(\bar{k}/k) \rightarrow \text{Aut}_{L_1}(T_0)$.

Since the torus T_0 is already split over k , we have $\text{Aut}_{L_1}(T_0) \cong \text{Aut}_k(T_0)$, and hence the Galois group $\text{Gal}(\bar{k}/k)$ acts trivially on $\text{Aut}_{L_1}(T_0)$, which is isomorphic to $\text{GL}_n(\mathbb{Z})$. Therefore, φ_f is actually a homomorphism from $\text{Gal}(\bar{k}/k)$ to $\text{GL}_n(\mathbb{Z})$. This is an n -dimensional integral representation of $\text{Gal}(\bar{k}/k)$. By changing the isomorphism f to any other L_1 -isomorphism from T_0 to T_1 , we get an equivalent 1-cocycle to φ_f . Thus the element $[\varphi_f]$ in $H^1(k, \text{GL}_n(\mathbb{Z}))$ is determined by T_1 and we denote it by $\varphi(T_1)$. Thus a k -isomorphism class of an n -dimensional

torus gives us an equivalence class of n -dimensional integral representations of the Galois group, $\text{Gal}(\bar{k}/k)$.

In the other direction, if $\rho : \text{Gal}(\bar{k}/k) \rightarrow \text{GL}_n(\mathbb{Z})$ is an integral Galois representation then ρ is a 1-cocycle as the Galois action on $\text{GL}_n(\mathbb{Z})$ is trivial. Then the torus obtained by twisting the split torus T_0 by the 1-cocycle ρ is the required torus ([36, §III 1.3]). \square

We now describe the conjugacy classes of a maximal torus in a reductive k -group using Galois cohomology. We state the result for split reductive k -groups, but it nevertheless holds for all reductive k -groups.

(II.7) Lemma. *Let H be a split, connected, semisimple algebraic group defined over a field k . Fix a split maximal torus T_0 in H and let $N(T_0)$ denote the normaliser of the torus T_0 in H . The natural embedding $N(T_0) \hookrightarrow H$ induces a map $\Psi : H^1(k, N(T_0)) \rightarrow H^1(k, H)$. The set of k -conjugacy classes of maximal tori in H are in one-one correspondence with the subset of $H^1(k, N(T_0))$ which is mapped to the neutral element in $H^1(k, H)$ under the map Ψ .*

Proof: Let T be a maximal k -torus in H and let L be a splitting field of T , i.e., assume that the torus T splits as a product of \mathbb{G}_m 's over L . We assume that the field L is Galois over k . By the uniqueness of maximal split tori up to conjugacy, there exists an element $a \in H(L)$ such that $aT_0a^{-1} = T$, where T_0 is the split maximal torus in H fixed before. Then for any $\sigma \in \text{Gal}(L/k)$, we have $\sigma(a)T_0\sigma(a)^{-1} = T$, as both T_0 and T are defined over k . This implies that

$$(a^{-1}\sigma(a)) T_0 (a^{-1}\sigma(a))^{-1} = T_0.$$

Therefore $a^{-1}\sigma(a) \in N(T_0)$. This enables us to define a map $\text{Gal}(L/k) \rightarrow N(T_0)$ which sends σ to $a^{-1}\sigma(a)$. By composing this map with the natural map $\text{Gal}(\bar{k}/k) \rightarrow \text{Gal}(L/k)$, we get a map $\phi_a : \text{Gal}(\bar{k}/k) \rightarrow N(T_0)$. One checks that

$$\phi_a(\sigma\tau) = \phi_a(\sigma)\sigma(\phi_a(\tau)) \quad \forall \sigma, \tau \in \text{Gal}(\bar{k}/k),$$

i.e., the map ϕ_a is a 1-cocycle. If $b \in H(L)$ is another element such that $bT_0b^{-1} = T$, we see that

$$\phi_a(\sigma) = (b^{-1}a)^{-1}\phi_b(\sigma)\sigma(b^{-1}a).$$

Thus the element $[\phi_a] \in H^1(k, N(T_0))$ is determined by the maximal torus T . We denote it by $\phi(T)$. It is clear that $\phi(T)$ is determined by the k -conjugacy class of T . Moreover, if $\phi(T) = \phi(S)$ for two maximal tori T and S in H , then one can check that these two tori are conjugate over k . Indeed, if $T = aT_0a^{-1}$ and $S = bT_0b^{-1}$ for $a, b \in H(\bar{k})$, then for any $\sigma \in \text{Gal}(\bar{k}/k)$,

$$a^{-1}\sigma(a) = c^{-1} (b^{-1}\sigma(b)) \sigma(c)$$

for some $c \in N(T_0)$. Then, $\sigma(bca^{-1}) = bca^{-1}$ for all $\sigma \in \text{Gal}(\bar{k}/k)$, hence bca^{-1} is an element of $H(k)$ and $(bca^{-1})T(bca^{-1})^{-1} = S$. Further, it is clear that the image of ϕ in $H^1(k, N(T_0))$ is mapped to the neutral element in $H^1(k, H)$ under the map Ψ .

Moreover, if a 1-cocycle $\phi_1 : \text{Gal}(\bar{k}/k) \rightarrow N(T_0)$ is such that $\Psi(\phi_1)$ is neutral in $H^1(k, H)$, then $\phi_1(\sigma) = a^{-1}\sigma(a)$ for some $a \in H(\bar{k})$. Then the cohomology class $[\phi_1] \in H^1(k, N(T_0))$ corresponds to the maximal torus $S_1 = aT_0a^{-1}$ in H . Since $a^{-1}\sigma(a) = \phi_1(\sigma) \in N(T_0)$, the torus S_1 is invariant under the Galois action, therefore we conclude that it is defined over k . Thus the image of ϕ is the inverse image of the neutral element in $H^1(k, H)$ under the map Ψ . This is the complete description of the k -conjugacy classes of maximal k -tori in the group H .

Finally, we observe that the detailed proof we have given above amounts to looking at the exact sequence $1 \rightarrow N(T_0) \rightarrow H \rightarrow H/N(T_0) \rightarrow 1$ which gives an exact sequence of pointed sets:

$$H/N(T_0)(k) \longrightarrow H^1(k, N(T_0)) \xrightarrow{\Psi} H^1(k, H).$$

Therefore $H/N(T_0)(k)$, which is the variety of conjugacy classes of k -tori in H , is identified to elements in $H^1(k, N(T_0))$ which become trivial in $H^1(k, H)$. \square

§9. Herbrand quotient.

If G is a finite cyclic group then the cohomology groups $H^i(G, A)$ for any G -module A depend only on the parity of i . Let $N_G = \sum_{g \in G} g$. Then the Tate's cohomology group $\hat{H}^0(G, A)$ is defined to be the quotient $A^G/N_G A$. We define the *Herbrand quotient*

$$h(A) = \frac{|\hat{H}^0(G, A)|}{|H^1(G, A)|}$$

whenever it is defined.

(II.8) Lemma ([35, Proposition VIII.8]). *If G is a cyclic group and A is a finite G -module, then $h(A) = 1$.*

(II.9) Lemma. *Let \mathbb{F}_q be the finite field of q elements and let A be a finite $\text{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q)$ -module, then*

$$|H^0(\mathbb{F}_q, A)| = |H^1(\mathbb{F}_q, A)|.$$

Proof: We fix the finite field \mathbb{F}_q and let G denote the absolute Galois group of \mathbb{F}_q , $\text{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q)$. Let A be a finite G -module. By the above lemma, it is enough to prove that the sets $\hat{H}^0(\mathbb{F}_q, A)$ and $H^0(\mathbb{F}_q, A)$ are the same.

Let G_n be the Galois group of the extension \mathbb{F}_{q^n} over \mathbb{F}_q and H_n be the Galois group of $\overline{\mathbb{F}_q}$ over \mathbb{F}_{q^n} , so that $G_n = G/H_n \xrightarrow{\sim} \mathbb{Z}/n\mathbb{Z}$. We have

$$\begin{aligned} H^0(\mathbb{F}_q, A) &= \varinjlim H^0(G_n, A^{H_n}) \\ &= \varinjlim (A^{H_n})^{G_n} \\ &= A^G \end{aligned}$$

and

$$\begin{aligned} \widehat{H}^0(\mathbb{F}_q, A) &= \varinjlim \widehat{H}^0(G_n, A^{H_n}) \\ &= \varinjlim (A^{H_n})^{G_n} / N_{G_n} A^{H_n} \\ &= \varinjlim A^G / N_{G_n} A^{H_n}. \end{aligned}$$

Every element of $g \in G_n$ has order n therefore the image of g under the natural map $: A^G / N_{G_n} A^{H_n} \rightarrow A^G / N_{G_{n^2}} A^{H_{n^2}}$ is zero. This holds for every G_n therefore we get the direct limit as

$$\varinjlim A^G / N_{G_n} A^{H_n} = A^G.$$

This proves the lemma. □

(II.10) Lemma. *Let H be a connected semisimple algebraic group defined over a finite field \mathbb{F}_q . If H_1 is a connected semisimple algebraic group defined over \mathbb{F}_q which is isogenous to H , then $|H(\mathbb{F}_q)| = |H_1(\mathbb{F}_q)|$.*

Proof: It is enough to prove that if \widetilde{H} is a simply connected group in the isogeny class of H then the order of $\widetilde{H}(\mathbb{F}_q)$ is the same as the order of $H(\mathbb{F}_q)$.

Let \widetilde{H} be the simply connected group isogenous to H . We have an exact sequence

$$0 \longrightarrow A \longrightarrow \widetilde{H} \longrightarrow H \longrightarrow 1$$

where A is a finite abelian group. We get the following exact sequence of Galois cohomology sets

$$0 \rightarrow H^0(\mathbb{F}_q, A) \rightarrow H^0(\mathbb{F}_q, \widetilde{H}) \rightarrow H^0(\mathbb{F}_q, H) \rightarrow H^1(\mathbb{F}_q, A) \rightarrow H^1(\mathbb{F}_q, \widetilde{H}).$$

By Lang's theorem, (II.4), $H^1(\mathbb{F}_q, \widetilde{H}) = 0$. Since all the sets in the above sequence are finite, we have

$$|H^0(\mathbb{F}_q, A)| \cdot |H^0(\mathbb{F}_q, H)| = |H^0(\mathbb{F}_q, \widetilde{H})| \cdot |H^1(\mathbb{F}_q, A)|.$$

Then it follows from the above lemma that

$$|H^0(\mathbb{F}_q, H)| = |H^0(\mathbb{F}_q, \widetilde{H})|, \text{ i.e., } |\widetilde{H}(\mathbb{F}_q)| = |H(\mathbb{F}_q)|.$$

□

CHAPTER III

Maximal tori determining the algebraic group

From now on, we start reporting on the research done by the author. This chapter reports the work done in [12]. The main theorem proved here is that the Weyl group of a connected, split, semisimple k -group H , where k is a number field, a local non-archimedean field or a finite field, is determined by the k -isomorphism classes of the maximal k -tori in H . Now onwards, we just say *arithmetic field* for a number field, a local non-archimedean field or a finite field.

In §10, we give the background of the main question and describe the proof in brief. The sections §11, 12 cover the basic material that is needed in the proof and the remaining sections of this chapter deal with the proof of the main theorem. We also present an easier proof of the theorem III.5 which was communicated to the author by Prof. T. A. Springer.

§10. Introduction.

It is a natural question to ask if a linear algebraic group is determined by the set of maximal tori in it. We study this question for connected, split, semisimple groups defined over arithmetic fields, i.e, over number fields, local non-archimedean fields and finite fields.

We prove (Theorem III.6) that the Weyl group of a split, connected, semisimple k -group H , where k is an arithmetic field, is determined by the k -isomorphism classes of the maximal tori in H . If we write the Weyl group, $W(H)$, as a direct product of the Weyl groups of simple direct factors of H , then these factors of $W(H)$ are also determined with their multiplicities. Since a split simple k -group is determined by its Weyl group, up to isogeny except for the groups of the type B_n and C_n , we get that the group H is determined up to isogeny except that we are not able to distinguish between the simple direct factors of H of the type B_n and C_n .

This result is the best possible result in some sense. From the explicit description of maximal k -tori in SO_{2n+1} and Sp_{2n} , see for instance [21, Proposition 2], one finds that the groups SO_{2n+1} and Sp_{2n} contain the same set of k -isomorphism classes of maximal k -tori.

We also show by an example that the existence of split tori in the group H is necessary. We know that the Brauer group of \mathbb{Q}_p is \mathbb{Q}/\mathbb{Z} . Consider the central

division algebras of degree five, say D_1 and D_2 , corresponding to $1/5$ and $2/5$ in \mathbb{Q}/\mathbb{Z} respectively. We now define two semisimple \mathbb{Q}_p -groups $H_1 = \mathrm{SL}_1(D_1)$ and $H_2 = \mathrm{SL}_1(D_2)$. The maximal tori in H_i correspond to the maximal commutative subfields in respective D_i . But over \mathbb{Q}_p , every division algebra of a fixed degree contains every field extension of that fixed degree ([33, Proposition 17.10 and Corollary 13.3]). Therefore, the groups H_1 and H_2 share the same set of maximal tori over k . But they are not isomorphic, since $\mathrm{SL}_1(D) \cong \mathrm{SL}_1(D')$ if and only if $D \cong D'$ or $D \cong (D')^{op}$ ([28, 26.11]).

We now give a brief information on how the proof goes. We have seen in the previous chapter, lemma (II.6) and lemma (II.7), that the k -isomorphism classes of n -dimensional k -tori and the k -conjugacy classes of maximal tori in a split reductive k -group can be computed using Galois cohomology. Using these two descriptions, we obtain a Galois cohomological description for the k -isomorphism classes of maximal tori in a split reductive k -group. We further prove that if the split, connected, semisimple algebraic groups of rank n , H_1 and H_2 , share the same set of maximal k -tori up to k -isomorphism, then the Weyl groups $W(H_1)$ and $W(H_2)$, considered as subgroups of $GL_n(\mathbb{Z})$, share the same set of elements up to conjugacy in $GL_n(\mathbb{Z})$. Then the proof boils down to proving the following result:

If the Weyl groups of two split, connected, semisimple algebraic groups, W_1 and W_2 , embedded in $GL_n(\mathbb{Z})$ in the natural way, i.e., by their action on the character group of a fixed split maximal torus, have the property that every element of W_1 is $GL_n(\mathbb{Z})$ -conjugate to one in W_2 , and vice versa, then the Weyl groups are isomorphic.

Our analysis finally depends on the knowledge of characteristic polynomials of elements in the Weyl groups considered as subgroups of $GL_n(\mathbb{Z})$. We would like to emphasize that if we were proving the result for simple algebraic groups, then our proof is relatively very simple. However, for semisimple groups, we have to make a somewhat complicated inductive argument on the maximal rank among the simple factors of the semisimple groups H_i .

We use the term *simple Weyl group of rank r* for the Weyl group of a simple algebraic group of rank r . Any Weyl group is a product of simple Weyl groups in a unique way (up to permutation). We say that two Weyl groups are isomorphic if and only if the simple factors and their multiplicities are the same.

This study seems relevant for the study of Mumford-Tate groups over algebraic number fields.

§11. Galois cohomological lemmas.

Let k denote an arbitrary field and let $\mathrm{Gal}(\bar{k}/k)$ be the Galois group of \bar{k} , the algebraic closure of k , over k . Let H denote a split, connected, semisimple

algebraic group defined over k and let T_0 be a fixed split maximal torus in H . Suppose that the dimension of T_0 is n . Let W be the Weyl group of H with respect to T_0 . Then we have an exact sequence of algebraic groups defined over k ,

$$0 \longrightarrow T_0 \longrightarrow N(T_0) \longrightarrow W \longrightarrow 1$$

where $N(T_0)$ denotes the normalizer of T_0 in H . This exact sequence induces a map $\psi : H^1(k, N(T_0)) \rightarrow H^1(k, W)$.

We have seen in lemma (II.7) that a certain subset of $H^1(k, N(T_0))$ classifies k -conjugacy classes of maximal tori in H . Since the group H is k -split, the Weyl group W is defined over k , and $W(\bar{k}) = W(k)$. Therefore $\text{Gal}(\bar{k}/k)$ acts trivially on W , and hence the elements of $H^1(k, W)$ correspond to the isomorphism classes of Galois representations with values in W . Since W acts faithfully on the character group of T_0 , we get that $W \hookrightarrow \text{GL}_n(\mathbb{Z})$ and this induces a map $i : H^1(k, W) \rightarrow H^1(k, \text{GL}_n(\mathbb{Z}))$.

Let T be an arbitrary maximal k -torus in H . This torus determines a unique element $\phi(T) \in H^1(k, N(T_0))$, guaranteed by lemma (II.7). The image of this element $\phi(T)$ under the map $i \circ \psi$ in $H^1(k, \text{GL}_n(\mathbb{Z}))$ associates an integral Galois representation to the torus T . But, we already have another integral Galois representation associated to the torus T , given by $\varphi(T) \in H^1(k, \text{GL}_n(\mathbb{Z}))$ (Lemma II.6). We prove that these two representations are equivalent.

(III.1) Lemma. *Let the notations be as above. For every maximal k -torus T in H , the integral representations given by $i \circ \psi \circ \phi(T)$ and $\varphi(T)$ are equivalent.*

Proof: The proof follows by carefully examining the definitions of the elements $i \circ \psi \circ \phi(T)$ and $\varphi(T)$.

If L is a splitting field of T , then an element $a \in H(L)$ such that $aT_0a^{-1} = T$ gives rise to a 1-cocycle $\phi_a : \text{Gal}(\bar{k}/k) \rightarrow N(T_0)$, $\sigma \mapsto a^{-1}\sigma(a)$ and $\phi(T)$ is precisely the element $[\phi_a] \in H^1(k, N(T_0))$. Further, we treat the conjugation by a as an L -isomorphism $f : T_0 \rightarrow T$, and then it can be checked that the map $f^\sigma := \sigma f \sigma^{-1}$ is the conjugation by $\sigma(a)$. The element $\varphi(T) \in H^1(k, \text{GL}_n(\mathbb{Z}))$ is equal to $[\varphi_f]$, where $\varphi_f(\sigma) = f^{-1}f^\sigma$.

Now, the map $\psi_1 : N(T_0) \rightarrow W$ is the natural map which takes $\alpha \in N(T_0)$ to $\bar{\alpha} := \alpha \cdot T_0 \in W = N(T_0)/T_0$. Hence we have

$$\psi_1(\phi_a(\sigma)) = \overline{a^{-1}\sigma(a)} = f^{-1}f^\sigma = \varphi_f(\sigma) \quad \forall \sigma \in \text{Gal}(\bar{k}/k).$$

Since the action of W on T_0 is given by conjugation, it is clear that the integral representations of the Galois group, $\text{Gal}(\bar{k}/k)$, given by $\psi(\phi(T))$ and $\varphi(T)$ are equivalent. \square

Thus, a k -isomorphism class of a maximal torus in H gives an integral Galois representation taking values in the Weyl group W . If all subgroups of the Weyl

group W could appear as the images of some integral Galois representation, then the Weyl group itself would be one such. Then it would be quite easy to determine the Weyl group as the largest subgroup of $\mathrm{GL}_n(\mathbb{Z})$ that appears as the image of some integral Galois representation associated to the maximal torus in H . Unfortunately, this is not the case. For instance, over finite fields the only finite images of the absolute Galois group are cyclic groups. However, we have following weaker result for finite fields and local non-archimedean fields.

(III.2) Lemma. *Let k be a finite field or a local non-archimedean field and let H, T_0, W be as above. An element in $H^1(k, W)$ which corresponds to a homomorphism $\rho : \mathrm{Gal}(\bar{k}/k) \rightarrow W$ with cyclic image, corresponds to the k -isomorphism class of some maximal k -torus in H under the mapping $\psi : H^1(k, N(T_0)) \rightarrow H^1(k, W)$.*

Proof: Consider the map $\Psi : H^1(k, N(T_0)) \rightarrow H^1(k, H)$ induced by the inclusion $N(T_0) \hookrightarrow H$. If we denote the neutral element in $H^1(k, H)$ by ι , then by lemma (II.7) the set

$$X := \{f \in H^1(k, N(T_0)) : \Psi(f) = \iota\}$$

is in one-one correspondence with the k -conjugacy classes of maximal tori in H . By the previous lemma, it is enough to show that $[\rho] \in \psi(X)$, where $\psi : H^1(k, N(T_0)) \rightarrow H^1(k, W)$ is induced by the natural map from $N(T_0)$ to W .

By Tits' theorem ([45, 4.6]), there exists a subgroup \bar{W} of $N(T_0)(k)$ such that the sequence

$$0 \longrightarrow \mu_2^n \longrightarrow \bar{W} \longrightarrow W \longrightarrow 1$$

is exact, where n is the dimension of the split torus $T_0 \subset H$. Let N denote the image of ρ in W . We know that N is a cyclic subgroup of W . Let w be a generator of N and let \bar{w} be a lifting of w to \bar{W} . Since the base field k admits cyclic extensions of any given degree, there exists a map ρ_1 from $\mathrm{Gal}(\bar{k}/k)$ to \bar{W} whose image is the cyclic subgroup generated by \bar{w} . Since the Galois action on \bar{W} is trivial, as \bar{W} is a subgroup of $N(T_0)(k)$, the map ρ_1 could be treated as a 1-cocycle from $\mathrm{Gal}(\bar{k}/k)$ to $N(T_0)$. Consider $[\rho_1]$ as an element in $H^1(k, N(T_0))$, then $\psi([\rho_1]) = [\rho] \in H^1(k, W)$. We have yet to show that $[\rho_1]$ is an element of X . We make two cases depending on the base field.

Case 1: k is a finite field. By Lang's theorem (II.4), $H^1(k, H)$ is trivial and hence the set X coincides with $H^1(k, N(T_0))$. Therefore the element $[\rho_1] \in H^1(k, N(T_0))$ corresponds to a k -conjugacy class of maximal k -torus in H . Then, by previous lemma, $[\rho] = \psi([\rho_1])$ corresponds to a k -isomorphism class of maximal k -tori in H .

Case 2: k is a local non-archimedean field. By theorem (I.4), there exists a semisimple simply connected algebraic group \tilde{H} , which is defined over k , together

with a k -isogeny $\pi : \tilde{H} \rightarrow H$. We have already fixed a split maximal torus T_0 in H , let \tilde{T}_0 be the split maximal torus in \tilde{H} which gets mapped to T_0 by the covering map π . It can be seen that, by restriction we get a surjective map $\pi : N(\tilde{T}_0) \rightarrow N(T_0)$, where the normalizers are taken in appropriate groups. Moreover, the induced map $\pi_1 : \tilde{W} \rightarrow W$ is an isomorphism.

We define the maps

$$\tilde{\psi} : H^1(k, N(\tilde{T}_0)) \rightarrow H^1(k, \tilde{W}) \quad \text{and} \quad \tilde{\Psi} : H^1(k, N(\tilde{T}_0)) \rightarrow H^1(k, \tilde{H})$$

in the same way as the maps ψ and Ψ are defined for the group H .

Consider the following diagrams,

$$\begin{array}{ccccc} \tilde{H} & \longleftarrow & N(\tilde{T}_0) & \longrightarrow & \tilde{W} \\ \pi \downarrow & & \pi \downarrow & & \downarrow \pi_1 \\ H & \longleftarrow & N(T_0) & \longrightarrow & W, \end{array}$$

$$\begin{array}{ccccc} H^1(k, \tilde{H}) & \xleftarrow{\tilde{\Psi}} & H^1(k, N(\tilde{T}_0)) & \xrightarrow{\tilde{\psi}} & H^1(k, \tilde{W}) \\ \pi^* \downarrow & & \pi^* \downarrow & & \downarrow \pi_1^* \\ H^1(k, H) & \xleftarrow{\Psi} & H^1(k, N(T_0)) & \xrightarrow{\psi} & H^1(k, W). \end{array}$$

The first diagram is clearly commutative and so is the other. Since π_1 is an isomorphism, the map π_1^* is a bijection. Now, consider an element $[\rho] \in H^1(k, W)$, such that the image of the 1-cocycle ρ is a cyclic subgroup of W , and let $[\tilde{\rho}]$ be its inverse image in $H^1(k, \tilde{W})$ under the bijection π_1^* . Using Tits' theorem ([45]) as above, we lift $[\tilde{\rho}]$ to an element $[\tilde{\rho}_1]$ in $H^1(k, N(\tilde{T}_0))$. Since \tilde{H} is simply connected and k is a non-archimedean local field, $H^1(k, \tilde{H})$ is trivial by Kneser's theorem (II.5). Therefore, $\tilde{\Psi}([\tilde{\rho}_1])$ is neutral in $H^1(k, \tilde{H})$ and so is $\pi^*(\tilde{\Psi}([\tilde{\rho}_1]))$ in $H^1(k, H)$. By commutativity of the diagram, we have that the element $[\rho] \in H^1(k, W)$ has a lift $\pi^*([\tilde{\rho}_1])$ in $H^1(k, N(T_0))$ such that $\Psi(\pi^*([\tilde{\rho}_1]))$ is neutral in $H^1(k, H)$. Thus the element $[\rho]$ corresponds to a k -isomorphism class of a maximal torus in H .

This proves the lemma. \square

§12. Reflection groups and characteristic polynomials.

This section is devoted to the study of the characteristic polynomials of the elements of Weyl groups, seen as subgroups of $\mathrm{GL}_n(\mathbb{Z})$.

We define a *complex reflection group* W to be a finite group generated by reflections, i.e., diagonalizable invertible matrices having all but one eigenvalues equal to 1, in some $\mathrm{GL}_n(\mathbb{C})$. The group W then acts in a natural way on the

ring of polynomial functions on $V = \mathbb{C}^n$. It is a fact that the subring of invariant polynomial functions, under the W -action, is generated by n homogeneous polynomials whose degrees depend only on the group W ([19, Theorem 3.5 and Proposition 3.7]). We call these degrees the *fundamental degrees* of the group W . A lot of information about the group W is hidden in these degrees. We quote a theorem by T. A. Springer, which will be used in the later sections of this chapter.

(III.3) Theorem (Springer [38]). *Let W be a complex reflection group and let d_1, \dots, d_m be the fundamental degrees of W . An r^{th} root of unity occurs as an eigenvalue for some element of W if and only if r divides one of the fundamental degrees d_i of W .*

For a finite subgroup W of $\text{GL}_n(\mathbb{Z})$, we define $ch(W)$ to be the set of characteristic polynomials of elements of W and $ch^*(W)$ to be the set of irreducible factors of elements of $ch(W)$. Since all the elements of W are of finite order, the irreducible factors (over \mathbb{Z}) of the characteristic polynomials $ch(x)$ are cyclotomic polynomials. We denote by ϕ_r , the r -th cyclotomic polynomial, i.e., the irreducible monic polynomial over \mathbb{Z} satisfied by a primitive r -th root of unity. Then

$$\begin{aligned} ch(W) &= \{ch(x) : x \in W \subset \text{GL}_n(\mathbb{Z})\}, \\ ch^*(W) &= \{\phi_r : \phi_r \text{ divides some } f \in ch(W)\}. \end{aligned}$$

We now restate the above mentioned theorem of Springer for Weyl groups:

(III.4) Theorem (Springer [38]). *Let W be a Weyl group embedded in some $\text{GL}_n(\mathbb{Z})$ in the natural way and let d_1, \dots, d_m denote the fundamental degrees of W . Then $\phi_r \in ch^*(W)$ if and only if r divides one of the fundamental degrees d_i of the reflection group W .*

We define

$$\begin{aligned} \mathbf{m}_i(W) &= \max \{t : \phi_i^t \text{ divides some } f \in ch(W)\}, \\ \mathbf{m}'_i(W) &= \min \{t : \phi_2^t \cdot \phi_i^{\mathbf{m}_i(W)} \text{ divides some } f \in ch(W)\}, \text{ and} \\ \mathbf{m}_{i,j}(W) &= \max \{t + s : \phi_i^t \cdot \phi_j^s \text{ divides some } f \in ch(W)\}. \end{aligned}$$

If U_1 is a subgroup of $\text{GL}_n(\mathbb{Z})$ and U_2 is a subgroup of $\text{GL}_m(\mathbb{Z})$, then $U_1 \times U_2$ can be treated as a subgroup of $\text{GL}_{m+n}(\mathbb{Z})$. Then

$$ch(U_1 \times U_2) = \{f_1 \cdot f_2 : f_1 \in ch(U_1), f_2 \in ch(U_2)\}.$$

Moreover, one can easily check that

$$\begin{aligned} \mathbf{m}_i(U_1 \times U_2) &= \mathbf{m}_i(U_1) + \mathbf{m}_i(U_2) \quad \forall i, \\ \mathbf{m}'_i(U_1 \times U_2) &= \mathbf{m}'_i(U_1) + \mathbf{m}'_i(U_2) \quad \forall i, \\ \mathbf{m}_{i,j}(U_1 \times U_2) &= \mathbf{m}_{i,j}(U_1) + \mathbf{m}_{i,j}(U_2) \quad \forall i, j. \end{aligned}$$

Therefore to obtain the sets $ch(W)$ and $ch^*(W)$ for all Weyl groups W , it is enough to obtain these sets for simple Weyl groups. A simple Weyl group W of rank n has a natural embedding in $GL_n(\mathbb{Z})$. We now list the fundamental degrees and the divisors of degrees for the simple Weyl groups, cf. [19, 3.7]:

Table 2

	Fundamental degrees	Divisors of degrees
A_n	$2, 3, \dots, n+1$	$1, 2, \dots, n+1$
B_n	$2, 4, \dots, 2n$	$1, 2, \dots, n, n+2, n+4, \dots, 2n$ n even
C_n	$2, 4, \dots, 2n$	$1, 2, \dots, n, n+1, n+3, \dots, 2n$ n odd
D_n	$2, 4, \dots, 2n-2, n$	$1, 2, \dots, n, n+2, n+4, \dots, 2n-2$ n even
		$1, 2, \dots, n, n+1, n+3, \dots, 2n-2$ n odd
G_2	$2, 6$	$1, 2, 3, 6$
F_4	$2, 6, 8, 12$	$1, 2, 3, 4, 6, 8, 12$
E_6	$2, 5, 6, 8, 9, 12$	$1, 2, 3, 4, 5, 6, 8, 9, 12$
E_7	$2, 6, 8, 10, 12, 14, 18$	$1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 14, 18$
E_8	$2, 8, 12, 14, 18, 20, 24, 30$	$1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 14, 15, 18, 20, 24, 30$

Using Springer's theorem (III.4) and the above table, we get the sets $ch^*(W)$ for all simple Weyl groups W . We do not distinguish between the Weyl groups $W(B_n)$ and $W(C_n)$ as they are isomorphic.

- (1) $ch^*(W(A_n)) = \{\phi_1, \phi_2, \dots, \phi_{n+1}\}$
- (2) $ch^*(W(B_n)) = \{\phi_i, \phi_{2i} : i = 1, 2, \dots, n\}$
- (3) $ch^*(W(D_n)) = \{\phi_i, \phi_{2j} : i = 1, 2, \dots, n, j = 1, 2, \dots, n-1\}$
- (4) $ch^*(W(G_2)) = \{\phi_1, \phi_2, \phi_3, \phi_6\}$
- (5) $ch^*(W(F_4)) = \{\phi_1, \phi_2, \phi_3, \phi_4, \phi_6, \phi_8, \phi_{12}\}$
- (6) $ch^*(W(E_6)) = \{\phi_1, \phi_2, \phi_3, \phi_4, \phi_5, \phi_6, \phi_8, \phi_9, \phi_{12}\}$
- (7) $ch^*(W(E_7)) = \{\phi_1, \phi_2, \dots, \phi_{10}, \phi_{12}, \phi_{14}, \phi_{18}\}$
- (8) $ch^*(W(E_8)) = \{\phi_1, \phi_2, \dots, \phi_{10}, \phi_{12}, \phi_{14}, \phi_{15}, \phi_{18}, \phi_{20}, \phi_{24}, \phi_{30}\}$

§13. Determining the Weyl groups.

In this section, we take an important step towards proving that the integers $\mathbf{m}_i(W)$, $\mathbf{m}'_i(W)$ and $\mathbf{m}_{i,j}(W)$ determine the Weyl group W up to isomorphism. This result is the heart of this chapter. Here we prove that the product of the simple Weyl groups of the highest rank in W is determined by the integers $\mathbf{m}_i(W)$, $\mathbf{m}'_i(W)$ and $\mathbf{m}_{i,j}(W)$.

(III.5) Theorem. *Let H_1 and H_2 be split, connected, semisimple algebraic groups of the same rank, say n , defined over a field k . Let W_1 and W_2 denote the respective Weyl groups of the groups H_1 and H_2 . Assume that*

$$\mathbf{m}_i(W_1) = \mathbf{m}_i(W_2), \quad \mathbf{m}'_i(W_1) = \mathbf{m}'_i(W_2), \quad \mathbf{m}_{i,j}(W_1) = \mathbf{m}_{i,j}(W_2) \quad \forall i, j.$$

Let m be the maximum possible rank among the simple factors of H_1 and H_2 . Let W'_i denote the product of the Weyl groups of simple factors of H_i of rank m for $i = 1, 2$. Then the groups W'_1 and W'_2 are isomorphic.

The proof of this theorem occupies the rest of this section. We distribute the proof over several subsections.

We prove this result by proving that if a simple Weyl group of rank m appears as a factor of W_1 with multiplicity p , then it appears as a factor of W_2 , with the same multiplicity. We use case by case analysis depending on the type of rank m simple factors of H_i .

The main idea here is to compare the sets $ch^*(W)$ for the simple Weyl groups of rank m . We observe from Table 2, that if we put the simple Weyl groups of rank m in the decreasing order according to their maximal fundamental degrees we get that the simple Weyl group of exceptional type, if any, comes first, then comes $W(B_m)$, the next one is $W(D_m)$ and finally the Weyl group $W(A_m)$ has the smallest maximal degree. So, we begin the proof with the case of exceptional groups of rank m , prove that it occurs with the same multiplicity for $i = 1, 2$. Once that is done, we prove the result for B_m , then for D_m and finally we prove the result for the group A_m .

13.A. Exceptional group of rank m . In this case, we assume that there exists a simple Weyl group of exceptional type of rank m , i.e., we assume that $m \in \{2, 4, 6, 7, 8\}$.

We first treat the case of the simple group E_8 , i.e., we assume that 8 is the maximum possible rank of the simple factors of the groups H_i . We know that $\mathbf{m}_{30}(W(E_8)) = 1$. Observe that ϕ_{30} is an irreducible polynomial of degree 8, hence it cannot occur in $ch^*(W)$ for any simple Weyl group of rank ≤ 7 . Moreover, from theorem (III.4) and the Table 2, it is clear that

$$\mathbf{m}_{30}(W(A_8)) = \mathbf{m}_{30}(W(B_8)) = \mathbf{m}_{30}(W(D_8)) = 0.$$

Hence the multiplicity of E_8 in H_i is given by $\mathbf{m}_{30}(W_i)$ which is the same for $i = 1, 2$.

Similarly for the simple algebraic group E_7 , we observe that $\mathbf{m}_{18}(W(E_7)) = 1$ and $\mathbf{m}_{18}(W) = 0$ for any simple Weyl group W of rank ≤ 7 . Then the multiplicity of E_7 in H_i is given by $\mathbf{m}_{18}(W_i)$ which is the same for $i = 1, 2$.

The case of E_6 is done by using \mathbf{m}_9 . It is clear that $\mathbf{m}_9(W) = 0$ for any simple Weyl group W of rank ≤ 6 .

The cases of F_4 and G_2 are done similarly by using \mathbf{m}_{12} and \mathbf{m}_6 respectively.

13.B. The groups B_m and C_m . Since $W(B_m) \cong W(C_m)$, we treat the case of B_m only. By §13.A, we can assume that the exceptional group of rank m , if any, occurs with the same multiplicities in both H_1 and H_2 , and hence while counting the multiplicities \mathbf{m}_i , \mathbf{m}'_i and $\mathbf{m}_{i,j}$, we can (and will) ignore the exceptional groups of rank m .

Observe that $\mathbf{m}_{2m}(W(B_m)) = 1$ and $\mathbf{m}_{2m}(W) = 0$ for any other simple Weyl group W of classical type of rank $\leq m$. However, it is possible that $\mathbf{m}_{2m}(W) \neq 0$ for a simple Weyl group W of exceptional type of rank strictly less than m . If $m \geq 16$, then this problem does not arise, therefore the multiplicity of B_m in H_i for $m \geq 16$ is given by $\mathbf{m}_{2m}(W_i)$, which is the same for $i = 1, 2$. We do the cases of B_m for $m \leq 15$ separately.

For the group B_2 , we observe that $\mathbf{m}_4(W(B_2)) = 1$ and $\mathbf{m}_4(W) = 0$ for any other simple Weyl group W of rank ≤ 2 . Thus, the case of B_2 is done using $\mathbf{m}_4(W_1) = \mathbf{m}_4(W_2)$.

For the group B_3 , we have $\mathbf{m}_6(W(B_3)) = 1$, but then $\mathbf{m}_6(W(G_2))$ is also 1. Observe that $\mathbf{m}_4(W(B_3)) = 1$ and $\mathbf{m}_4(W(G_2)) = 0$. Now, let the multiplicities of B_3 , G_2 and B_2 in the groups H_i be p_i , q_i and r_i , for $i = 1, 2$ respectively. Since, here we concentrate on \mathbf{m}_4 , \mathbf{m}_6 and $\mathbf{m}_{4,6}$, we do not have to worry about the simple Weyl groups W of rank ≤ 3 for which the multiplicities $\mathbf{m}_4(W)$ and $\mathbf{m}_6(W)$ are both zero. Then we get

$$\begin{aligned} p_1 + q_1 &= \mathbf{m}_6(W_1) = \mathbf{m}_6(W_2) = p_2 + q_2, \\ p_1 + r_1 &= \mathbf{m}_4(W_1) = \mathbf{m}_4(W_2) = p_2 + r_2 \end{aligned}$$

and

$$p_1 + q_1 + r_1 = \mathbf{m}_{4,6}(W_1) = \mathbf{m}_{4,6}(W_2) = p_2 + q_2 + r_2.$$

Combining these equalities, we get that $p_1 = p_2$, i.e., the group B_3 appears in both the groups H_i with the same multiplicity.

For the group B_4 , we observe that $\mathbf{m}_8(W(B_4)) = 1$. Since ϕ_8 has degree 4, it cannot occur in $ch(W)$ for any simple Weyl group of rank ≤ 3 and $\mathbf{m}_8(W(A_4)) = \mathbf{m}_8(W(D_4)) = 0$. Since we are assuming by §13.A that the group F_4 occurs in both H_i with the same multiplicity, we are done in this case also.

For the group B_5 , we have $\mathbf{m}_{10}(W(B_5)) = 1$ and $\mathbf{m}_{10}(W) = 0$ for any other simple Weyl group of classical type of rank ≤ 5 . Since 5 does not divide the order of $W(G_2)$ or $W(F_4)$, $\mathbf{m}_{10}(W(G_2)) = \mathbf{m}_{10}(W(F_4)) = 0$ and so we are done.

The group B_6 is another group where the exceptional groups give problems. We have $\mathbf{m}_{12}(W(B_6)) = 1$, but $\mathbf{m}_{12}(W(F_4))$ is also 1. We observe that $\mathbf{m}_{10}(W(B_6)) = 1$, but $\mathbf{m}_{10}(W(F_4)) = 0$. Now, let the multiplicities of B_6 , D_6 , B_5 and F_4 in H_i be p_i , q_i , r_i and s_i respectively. Then,

$$p_1 + s_1 = \mathbf{m}_{12}(W_1) = \mathbf{m}_{12}(W_2) = p_2 + s_2.$$

Similarly comparing \mathfrak{m}_{10} , we get that

$$p_1 + q_1 + r_1 = p_2 + q_2 + r_2.$$

Then, we compare $\mathfrak{m}_{10,12}$ of the groups W_1 and W_2 , to get that

$$p_1 + q_1 + r_1 + s_1 = p_2 + q_2 + r_2 + s_2.$$

Combining this equality with the one obtained by \mathfrak{m}_{10} , we get that $s_1 = s_2$ and hence $p_1 = p_2$. Thus the group B_6 occurs in both H_1 and H_2 with the same multiplicity.

We have that $\mathfrak{m}_{14}(W(E_6)) = 0$, therefore the group B_7 is characterized by ϕ_{14} and hence it occurs in both H_i with the same multiplicity.

For the group B_8 , $\mathfrak{m}_{16}(W(B_8)) = 1$. Since ϕ_{16} has degree 8, it cannot occur in $ch^*(W)$ for any of the Weyl groups of G_2, F_4, E_6 or E_7 . Thus, the group B_8 is characterized by ϕ_{16} and hence it occurs in both H_i with the same multiplicity.

The group B_9 has the property that $\mathfrak{m}_{18}(W(B_9)) = 1$. But we also have that $\mathfrak{m}_{18}(W(E_7)) = \mathfrak{m}_{18}(W(E_8)) = 1$. We conclude that the multiplicity of E_8 is the same for both W_1 and W_2 using \mathfrak{m}_{30} . Then we compare the multiplicities \mathfrak{m}_{18} , \mathfrak{m}_{16} and $\mathfrak{m}_{16,18}$ to prove that the group B_9 occurs in both the groups H_i with the same multiplicity.

Now, we do the case of B_{10} . Here $\mathfrak{m}_{20}(W(B_{10})) = 1$. Observe that $\mathfrak{m}_{20}(W) = 0$, for any other simple Weyl group W of rank ≤ 10 , except for E_8 . Then the multiplicity of B_{10} in H_i is $\mathfrak{m}_{20}(W_i) - \mathfrak{m}_{30}(W_i)$ and hence it is the same for $i = 1, 2$.

The same method works for B_{12} also, i.e. the multiplicity of B_{12} in H_i is $\mathfrak{m}_{24}(W_i) - \mathfrak{m}_{30}(W_i)$.

The multiplicities of B_{11}, B_{13} and B_{14} in H_i are given by $\mathfrak{m}_{22}(W_i), \mathfrak{m}_{26}(W_i)$ and $\mathfrak{m}_{28}(W_i)$ and hence they are the same for $i = 1, 2$. Now we are left with the case of B_{15} only.

For B_{15} , we have $\mathfrak{m}_{30}(W(B_{15})) = \mathfrak{m}_{30}(W(E_8)) = 1$ and it is 0 for any other simple Weyl group of rank ≤ 15 . Observe that $\mathfrak{m}_{28}(W(B_{15})) = \mathfrak{m}_{28}(W(B_{14})) = 1$ and it is 0 for any other simple Weyl group of rank ≤ 15 . Then by comparing \mathfrak{m}_{30} , \mathfrak{m}_{28} and $\mathfrak{m}_{28,30}$ we get the desired result that B_{15} occurs in both H_i with the same multiplicity.

13.C. The group D_m . While doing the case of D_m , we assume that the exceptional group of rank m , if any, and the group B_m occur in both H_i with the same multiplicities.

We observe that $2m - 2$ is the largest integer r such that $\phi_r \in ch^*(W(D_m))$, but $\mathfrak{m}_{2m-2}(W(B_{m-1})) = 1$. Hence we always have to compare the group D_m with the group B_{m-1} .

Let us assume that $m \geq 17$, so that $\phi_{2m-2} \notin ch^*(W)$ for any simple Weyl group of exceptional type of rank $< m$.

We know that $\mathfrak{m}_{2m-2}(W(D_m)) = \mathfrak{m}_{2m-2}(W(B_{m-1})) = 1$ and for any other simple Weyl group W of classical type of rank $\leq m$, $\mathfrak{m}_{2m-2}(W) = 0$. Further, $(X+1)(X^{m-1}+1)$ is the only element in $ch(W(D_m))$ which has ϕ_{2m-2} as a factor. Similarly $X^{m-1}+1$ is the only element in $ch(W(B_{m-1}))$ which has ϕ_{2m-2} as a factor. Observe that

$$\mathfrak{m}'_{2m-2}(W(D_m)) = \mathfrak{m}'_{2m-2}(W(B_{m-1})) + 1$$

and $\mathfrak{m}'_{2m-2}(W) = 0$ for any other simple Weyl group W of rank $\leq m$. Now, let p_i and q_i be the multiplicities of the groups D_m and B_{m-1} in H_i for $i = 1, 2$ respectively. Then by considering \mathfrak{m}_{2m-2} , we have

$$p_1 + q_1 = p_2 + q_2.$$

Further if m is even, then by considering \mathfrak{m}'_{2m-2} we have

$$2p_1 + q_1 = 2p_2 + q_2.$$

This equality, combined with the previous equality, implies that $p_1 = p_2$. If m is odd then \mathfrak{m}'_{2m-2} itself gives that $p_1 = p_2$. Thus, we get the result that the group D_m appears in both H_i with the same multiplicity for $i = 1, 2$.

Now we do the cases of D_m , for $m \leq 16$.

For the group D_4 , we have to consider the simple algebraic groups B_3 and G_2 . Comparing the multiplicities \mathfrak{m}_6 , \mathfrak{m}_4 and $\mathfrak{m}_{4,6}$ we get that G_2 occurs in both H_i with the same multiplicity, and then we proceed as above to prove that D_4 also occurs with the same multiplicity in both the groups H_i .

For the group D_5 , we first prove that the multiplicity of F_4 is the same for both H_i using \mathfrak{m}_{12} and then prove the required result by considering \mathfrak{m}_5 , \mathfrak{m}_8 and $\mathfrak{m}_{5,8}$. Now, while dealing the case of D_6 , we observe that $\mathfrak{m}_{10}(W(G_2)) = \mathfrak{m}_{10}(W(F_4)) = 0$, and so we do this case as done above for $m \geq 17$. The case of D_7 is done by considering \mathfrak{m}_7 , \mathfrak{m}_{12} and $\mathfrak{m}_{7,12}$.

While doing the case of D_8 , we first prove that the group E_7 occurs in both the H_i with the same multiplicity by considering \mathfrak{m}_{18} and then proceed as above. For the group D_9 , we prove that E_8 occurs in both H_i with the same multiplicity by considering \mathfrak{m}_{30} and proceed as done above for $m \geq 17$. While doing the case D_{10} , we prove that E_8 appears in both the H_i with the same multiplicity by considering \mathfrak{m}_{30} and the same can be proved for E_7 by considering \mathfrak{m}_{18} , \mathfrak{m}_{16} and $\mathfrak{m}_{16,18}$. Then we do this case as done above.

For the groups D_m , $m \geq 11$, the only simple Weyl group W of exceptional type such that $\phi_{2m-2} \in ch^*(W)$ is $W(E_8)$, but for D_m , $m \leq 15$, we can assume that E_8 occurs in both the H_i with the same multiplicity by considering \mathfrak{m}_{30} and hence we are through. For the group D_{16} , we take care of E_8 by considering \mathfrak{m}_{30} , \mathfrak{m}_{28} and $\mathfrak{m}_{28,30}$. Other arguments are the same as done in the case $m \geq 17$.

13.D. The group A_m . Now we do the last case, the case of simple algebraic group of type A_m . Here, as usual, we assume that all other simple algebraic groups of rank m occur with the same multiplicities in both H_i .

If m is even, then $m+1$ is odd and hence $\mathbf{m}_{m+1}(W) = 0$, for any simple Weyl group W of classical type of rank $< m$. If $m \geq 30$, then we do not have to bother about the exceptional simple groups of rank $< m$. If m is odd and $m \geq 31$, then ϕ_{m+1} occurs in $ch^*(W(B_r))$ and $ch^*(W(D_{r+1}))$ for $r \geq (m+1)/2$. Then we compare the multiplicities \mathbf{m}_m , \mathbf{m}_{m+1} and $\mathbf{m}_{m,m+1}$ and get the result that the group A_m occurs in H_i with the same multiplicity. So, we have to do the case of A_m for $m \leq 29$, separately.

The cases of A_1, A_2 are easy since there are no exceptional groups of rank 1. For A_3 , we use $\mathbf{m}_3, \mathbf{m}_4$ and $\mathbf{m}_{3,4}$ to get the result. Similarly A_4 is done by using \mathbf{m}_5 .

The problem comes for A_5 , since $\mathbf{m}_6(W(B_3)) \neq 0$, $\mathbf{m}_6(W(G_2)) \neq 0$ and $\mathbf{m}_6(W(F_4)) \neq 0$. But, this is handled by first proving that F_4 appears with the same multiplicity using \mathbf{m}_{12} and then using the multiplicities \mathbf{m}_5 , \mathbf{m}_6 and $\mathbf{m}_{5,6}$. The case of A_6 is done by using \mathbf{m}_7 . For A_7 , we use \mathbf{m}_7 , \mathbf{m}_8 and $\mathbf{m}_{7,8}$.

While doing the case of A_8 , we can first assume that the multiplicity of E_7 is the same for both H_i , by using \mathbf{m}_{18} . Then we use \mathbf{m}_7 , \mathbf{m}_9 and $\mathbf{m}_{7,9}$ to get the result. For the group A_9 , we can again get rid of E_7 and E_8 using the multiplicities \mathbf{m}_{18} and \mathbf{m}_{30} . Then we are left with the groups B_5 and E_6 , so here we work with \mathbf{m}_7 , \mathbf{m}_{10} and $\mathbf{m}_{7,10}$ to get the result.

Further, we observe that for $m \in \{10, 12, \dots, 28\}$ such that $m \neq 14$, we have that $\mathbf{m}_{m+1}(W) = 0$ for any simple Weyl group of rank $< m$. Thus, the multiplicities of the groups A_m , where $m \in \{10, 12, \dots, 28\}$ and $m \neq 14$, in H_i are characterized by considering $\mathbf{m}_{m+1}(W_i)$ and hence they are same for $i = 1, 2$. The case of A_{14} is done by using \mathbf{m}_{13} , \mathbf{m}_{15} and $\mathbf{m}_{13,15}$.

Thus, the only remaining cases are A_m where m is odd and $11 \leq m \leq 29$. We observe that for $m \in \{11, 13, \dots, 29\}$ such that $m \neq 15$, we have that the only simple Weyl group W of rank less than m such that $\mathbf{m}_m(W) \neq 0$ is A_{m-1} . Moreover, $\mathbf{m}_{m+1}(W(A_{m-1})) = 0$, so the cases of the groups A_m for $m \in \{11, 13, \dots, 29\}$, $m \neq 15$ is done by considering \mathbf{m}_m , \mathbf{m}_{m+1} and $\mathbf{m}_{m,m+1}$.

Thus, the only remaining case is that of A_{15} which can be done by considering \mathbf{m}_{13} , \mathbf{m}_{16} and $\mathbf{m}_{13,16}$.

This proves the required result.

§14. Main result.

Notations: We fix some notations for this section. Let k denote an arithmetic field, i.e., a number field, a local non-archimedean field or a finite field. We fix two split, connected, semisimple algebraic groups H_1 and H_2 defined over the

field k which share the same set of maximal k -tori up to k -isomorphism, i.e., for every maximal k -torus $T_1 \subset H_2$ there exists a maximal k -torus $T_2 \subset H_2$ such that the torus T_2 is k -isomorphic to T_1 and vice versa. We let $W_1 := W(H_1)$ and $W_2 := W(H_2)$.

We now state the main theorem.

(III.6) Theorem. *Let k, H_1, H_2, W_1 and W_2 be as above. Then the Weyl groups W_1 and W_2 are isomorphic. Moreover, if we write the Weyl groups W_1 and W_2 as a direct product of simple Weyl groups,*

$$W_1 = \prod_{\Lambda_1} W_{1,\alpha}, \quad \text{and} \quad W_2 = \prod_{\Lambda_2} W_{2,\beta},$$

then there exists a bijection $i : \Lambda_1 \rightarrow \Lambda_2$ such that $W_{1,\alpha}$ is isomorphic to $W_{2,i(\alpha)}$ for every $\alpha \in \Lambda_1$.

Since a split simple algebraic group with trivial center is determined by its Weyl group, except for the groups of the type B_n and C_n , we have following theorem.

(III.7) Theorem. *Let k, H_1, H_2 be as above and assume further that the groups H_1 and H_2 are adjoint. Write H_i as a direct product of simple (adjoint) groups,*

$$H_1 = \prod_{\Lambda_1} H_{1,\alpha}, \quad \text{and} \quad H_2 = \prod_{\Lambda_2} H_{2,\beta}.$$

There is a bijection $i : \Lambda_1 \rightarrow \Lambda_2$ such that $H_{1,\alpha}$ is isomorphic to $H_{2,i(\alpha)}$, except for the case when $H_{1,\alpha}$ is a simple group of type B_n or C_n , in which case $H_{2,i(\alpha)}$ could be of type C_n or B_n .

Clearly, the above mentioned groups H_1 and H_2 are of the same rank, say n . We therefore treat the Weyl groups W_1 and W_2 as subgroups of $\text{GL}_n(\mathbb{Z})$. We first transfer the information about the k -isomorphism classes of maximal tori in H_i to the one about the $\text{GL}_n(\mathbb{Z})$ -conjugacy classes of elements of the Weyl groups.

(III.8) Lemma. *Let W_1 and W_2 be as above. Then for every element $w_1 \in W_1$ there exists an element $w_2 \in W_2$ such that w_2 is conjugate to w_1 in $\text{GL}_n(\mathbb{Z})$ and vice versa.*

Proof: Let $w_1 \in W_1$ and let N_1 denote the subgroup of W_1 generated by w_1 . Since the base field k admits any cyclic group as a Galois group, there is a map $\rho_1 : \text{Gal}(\bar{k}/k) \rightarrow W_1$ such that $\rho_1(\text{Gal}(\bar{k}/k)) = N_1$.

We first consider the case when k is a finite field or a local non-archimedean field. By lemma (III.2), the element $[\rho_1] \in H^1(k, W_1)$ corresponds to a maximal k -torus in H_1 , say T_1 . Since the groups H_1 and H_2 share the same set of k -tori up to k -isomorphism, there exists a torus $T_2 \subset H_2$ which is k -isomorphic to T_1 . Then

lemma (III.1) gives us an integral Galois representation $\rho_2 : \text{Gal}(\bar{k}/k) \rightarrow \text{GL}_n(\mathbb{Z})$ corresponding to the k -isomorphism class of T_2 which factors through W_2 . Let $N_2 := \rho_2(\text{Gal}(\bar{k}/k)) \subseteq W_2$. Since T_1 and T_2 are k -isomorphic tori, the corresponding Galois representations, ρ_1 and ρ_2 , are equivalent. This implies that there exists $g \in \text{GL}_n(\mathbb{Z})$ such that $N_2 = gN_1g^{-1}$. Then $w_2 := gw_1g^{-1} \in N_2 \subseteq W_2$ is a conjugate of w_1 in $\text{GL}_n(\mathbb{Z})$. We can start with an element $w_2 \in W_2$ and obtain its $\text{GL}_n(\mathbb{Z})$ -conjugate in W_1 in the same way.

Now we consider the case when k is a number field. Let v be a non-archimedean valuation of k and let k_v be the completion of k with respect to v . Clearly the groups H_1 and H_2 are defined over k_v . Let $T_{1,v}$ be a maximal k_v -torus in H_1 . Then by Grothendieck's theorem ([5, 7.9 and 7.11]) and weak approximation property ([34, Proposition 7.3]), there exists a k -torus in H , say T_1 , such that $T_{1,v}$ is obtained from T_1 by the base change. By hypothesis, we have a k -torus T_2 in H_2 which is k -isomorphic to T_1 . Then the torus $T_{2,v}$, obtained from T_2 by the base change, is k_v -isomorphic to $T_{1,v}$. Thus, every maximal k_v -torus in H_1 has a k_v -isomorphic torus in H_2 . Similarly, we can show that every maximal k_v -torus in H_2 has a k_v -isomorphic torus in H_1 . Then, the proof follows by previous case. \square

(III.9) Corollary. *Let W_1 and W_2 be as above. Then $ch(W_1) = ch(W_2)$ and $ch^*(W_1) = ch^*(W_2)$. In particular, $\mathfrak{m}_i(W_1) = \mathfrak{m}_i(W_2)$, $\mathfrak{m}'_i(W_1) = \mathfrak{m}'_i(W_2)$ and $\mathfrak{m}_{i,j}(W_1) = \mathfrak{m}_{i,j}(W_2)$ for all i, j .*

Proof: Since the Weyl groups W_1 and W_2 share the same set of elements up to conjugacy in $\text{GL}_n(\mathbb{Z})$, the sets $ch(W_i)$ are the same for $i = 1, 2$, and hence the sets $ch^*(W_i)$ are also the same for $i = 1, 2$.

Further, for a fixed integer i , $\phi_i^{\mathfrak{m}_i(W_1)}$ divides an element $f_1 \in ch(W_1)$. But since $ch(W_1) = ch(W_2)$, the polynomial $\phi_i^{\mathfrak{m}_i(W_1)}$ divides some $f_2 \in ch(W_2)$ as well. Therefore $\mathfrak{m}_i(W_1) \leq \mathfrak{m}_i(W_2)$. We obtain the inequality in the other direction in the same way and hence $\mathfrak{m}_i(W_1) = \mathfrak{m}_i(W_2)$. Similarly, we can prove that $\mathfrak{m}'_i(W_1) = \mathfrak{m}'_i(W_2)$ and for integers i, j , $\mathfrak{m}_{i,j}(W_1) = \mathfrak{m}_{i,j}(W_2)$. \square

We now prove theorem (III.6), the main theorem.

Proof of theorem III.6: We recall that W_1 and W_2 denote the Weyl groups of H_1 and H_2 , respectively. It is clear from the corollary (III.9) that $\mathfrak{m}_i(W_1) = \mathfrak{m}_i(W_2)$, $\mathfrak{m}'_i(W_1) = \mathfrak{m}'_i(W_2)$ and $\mathfrak{m}_{i,j}(W_1) = \mathfrak{m}_{i,j}(W_2)$ for any i, j . Let m_0 be the maximum possible among the ranks of simple factors of the groups H_i . We apply the theorem (III.5) to conclude that the product of rank m_0 simple factors in W_i is isomorphic for $i = 1, 2$.

Let m be a positive integer less than m_0 . For $i = 1, 2$, let W'_i be the subgroup of W_i which is the product of the Weyl groups of simple factors of H_i of rank $> m$. We assume that the groups W'_1 and W'_2 are isomorphic and then we prove that

the product of the Weyl groups of rank m simple factors of H_i are isomorphic for $i = 1, 2$. This will complete the proof of the theorem by induction argument.

Let U_i be the direct product of the Weyl groups of simple direct factors of H_i of rank $\leq m$ so that $W_i = U_i \times W'_i$. Then, since $\mathfrak{m}_j(W'_1) = \mathfrak{m}_j(W'_2)$ and $\mathfrak{m}'_j(W'_1) = \mathfrak{m}'_j(W'_2)$, we have

$$\mathfrak{m}_j(U_1) = \mathfrak{m}_j(W_1) - \mathfrak{m}_j(W'_1) = \mathfrak{m}_j(W_2) - \mathfrak{m}_j(W'_2) = \mathfrak{m}_j(U_2),$$

$$\mathfrak{m}'_j(U_1) = \mathfrak{m}'_j(W_1) - \mathfrak{m}'_j(W'_1) = \mathfrak{m}'_j(W_2) - \mathfrak{m}'_j(W'_2) = \mathfrak{m}'_j(U_2)$$

and similarly

$$\mathfrak{m}_{i,j}(U_1) = \mathfrak{m}_{i,j}(U_2).$$

Then we apply theorem (III.5) for U_i to conclude that the subgroups of W_i which are products of the Weyl groups of simple factors of H_i of rank m are isomorphic for $i = 1, 2$.

The proof of the theorem can now be completed by the downward induction on m .

It also follows from the proof of the theorem (III.5), that the Weyl groups of simple factors of H_i are pairwise isomorphic. \square

§15. Another proof of Theorem III.5.

We now give another proof of the theorem (III.5) communicated to the author by Prof. T. A. Springer. This proof is much simpler than the one given in §13. The author thanks him for his permission to write the proof here.

The notations are as in [6].

1. Let W be a Weyl group, acting in the n -dimensional vector space V over \mathbb{C} (it is convenient to extend coefficients to \mathbb{C}). For each conjugacy class γ in G let f_γ be the characteristic polynomial of an element of γ (viewed as a linear map of V). Let \mathcal{F} be the family of polynomials (f_γ) , γ running through the conjugacy classes of W . The following result is proved in [12].

Proposition. *W is determined up to a linear isomorphism by \mathcal{F} .*

The proof given in [loc. cit.] uses explicit results about conjugacy classes in Weyl groups. Below is another proof, exploiting the properties of Coxeter elements.

2. First some recollections. Denote by d_1, \dots, d_n the characteristic degrees of W . Let ζ be a primitive root of unity of order d . For $w \in W$ let $V(w, \zeta)$ be the ζ -eigenspace of w . We have the following result (see [38, 3.4]).

Lemma 1. (i) $a(d) = \max_{w \in W} \dim V(w, \zeta)$ equals the number of d_i divisible by d ;

(ii) The spaces $V(w, \zeta)$ of dimension $a(d)$ form one W -orbit.

This has the following consequence.

Lemma 2. \mathcal{F} determines the degrees of W .

Proof. It follows from the previous lemma that the integers $a(d)$ are determined by \mathcal{F} . But these integers determine the degrees (as is easily seen).

Assume W to be irreducible. Denote by h the maximum of the degrees d_i and let $\zeta_h = e^{\frac{2\pi i}{h}}$.

Lemma 3. (i) h occurs only once among the d_i ;

(ii) The elements $c \in W$ with eigenvalue ζ_h form one conjugacy class;

(iii) The eigenvalues of c as in (ii) are $(\zeta_h^{d_i-1})_{1 \leq i \leq n}$. In particular: c has no eigenvalue 1.

For (i) and (iii) see [6, Ch. V, 6.2] and for (ii) [38, 4.2].

Now let again W be arbitrary. Then W is a direct product $W = W_1 \times \dots \times W_a$ of irreducible Weyl groups. There is a direct sum decomposition

$$V = V_1 \oplus \dots \oplus V_a$$

such that W_i acts trivially in the V_j with $j \neq i$ and acts as an irreducible Weyl group in V_i .

Let now h be the maximum of the Coxeter numbers of the W_i . It follows from Lemmas 1 and 3 that h is the maximal degree of W . By Lemma 2 h is determined by \mathcal{F} . Assume that W_1, \dots, W_b are the W_i with Coxeter number h . Put $W' = W_1 \times \dots \times W_b$, $W'' = W_{b+1} \times \dots \times W_a$. Then $W = W' \times W''$ and we have a corresponding decomposition $V = V' \oplus V''$.

Lemma 4. Assume that all W_i have the same Coxeter number h (i.e. $W = W'$). Then W is determined up to linear isomorphism by its degrees.

Proof. We use a number of explicit results contained in [6], in particular the description of the degrees for the various types.

If $h = 2$ the all W_i are of type A_1 and the Lemma is obvious. So assume $h > 2$.

A Coxeter number h occurs in the following classical types:

A_{h-1} , (if h is even) $B_{\frac{1}{2}h}$ and $D_{\frac{1}{2}h+1}$ (notice that the Weyl groups of types B_l and C_l are isomorphic).

In the exceptional types E_6, E_7, E_8, F_4, G_2 the Coxeter numbers are, respectively, 12, 18, 30, 12, 6.

Inspection of the lists of degrees for the various irreducible Weyl groups shows that the number of W_i of type A_{h-1} equals the multiplicity m of 3 in the set of degrees of W . Write $W \simeq (S_h)^m \times W_1$, where W_1 has no factor of type A . The degrees of W_1 can be read off from the degrees of W . If $m > 0$ an induction shows that W_1 is unique up to isomorphism.

So we may assume that W has no factors of type A . Then h is even and the number of factors of type $B_{\frac{1}{2}h}$ or $D_{\frac{1}{2}h+1}$ equals the multiplicity of 4 in the set of degrees. We can then reduce the proof to the two cases that the factors of W are either of exceptional type or are of type B and D .

In the first case the number of factors of type E_6 equals the multiplicity of 5 in the set of degrees. Discarding those factors we are left with the case that all factors are of one of the types E_7, E_8, F_4, G_2 . These cases are distinguished by the value of the Coxeter number h .

Finally, if only types B and D occur the degrees are $2, 4, \dots, h$, each with the same multiplicity and $\frac{1}{2}h + 1$ with multiplicity equal to the number of factors of type D . The number of factors of type B is then also determined.

This finishes the proof of Lemma 4.

We return to the general case. For $1 \leq i \leq b$ let c_i be a Coxeter element of W_i (of order h). Define $c \in W'$ by $c = (c_1, \dots, c_b)$ and let f be its characteristic polynomial, as a linear map of V' . Let \mathcal{F}'' be the set of characteristic polynomials for the Weyl group W'' , acting in V'' .

Lemma 5. *The characteristic polynomials of the elements $w \in W$ such that $\dim V(w, \zeta_h) = a(h)$ are the polynomials of the form fg where $g \in \mathcal{F}''$.*

Proof. Let $w'' \in W''$. Using part (iii) of Lemma 3 one sees that

$$\dim V((c, w''), \zeta_h) = b = a(h).$$

Now let $w = (w', w'')$ be such that $\dim V(w, \zeta_h) = b$. It follows from part (i) of Lemma 1 that w'' cannot have an eigenvalue ζ_h . Hence w' has an eigenvalue ζ_h with multiplicity b . Write $w' = (c'_1, \dots, c'_b)$, where $c'_i \in W_i$. Then c'_i must have an eigenvalue ζ_h in V_i , hence is conjugate to c_i in W_i . So w' is conjugate to c in W' . It follows that the characteristic polynomial of w is asserted.

We can now prove the proposition. By Lemma 5 there is a unique polynomial in \mathcal{F} which has a root ζ_h with multiplicity b and a maximal number of eigenvalues 1, viz. $f(t)(t - 1)^{\dim V''}$. By part (iii) of Lemma 3 f determines the degrees of W' . Lemma 4 then shows the uniqueness of W' . Lemma 5 describes the set \mathcal{F}'' . By an induction on the order of W we may assume that the uniqueness of W'' has been established. The Proposition follows.

Notes.

We remark here that theorem (III.5) holds even if we assume that the Weyl groups $W(H_1)$ and $W(H_2)$ share the same set of elements up to conjugacy in $\mathrm{GL}_n(\mathbb{C})$, not just in $\mathrm{GL}_n(\mathbb{Z})$. Thus theorem (III.6) is true under the weaker

assumption that the groups H_1 and H_2 share the same set of maximal k -tori up to k -isogeny, not just up to k -isomorphism.

Philippe Gille has recently proved ([15]) that the map ψ , described in lemma (III.1), is surjective for any quasisplit semisimple group H . Therefore our main theorem, Theorem (III.6), now holds for all fields k which admit cyclic extensions of arbitrary degree.

CHAPTER IV

Orders of finite semisimple groups

This chapter reports the work done in [13]. Here we investigate the extent to which a simply connected algebraic group H defined over a finite field \mathbb{F}_q is determined by the order of the finite group $H(\mathbb{F}_q)$. We describe the background of this study in §16, cover the basic material in §17 and the other sections describe the main work.

§16. Finite semisimple groups.

The theory of finite simple groups has enjoyed the attention of several mathematicians over decades. Emil Artin investigated if a finite simple group is determined by its order. He proved in [2, 3] that if H_1 and H_2 are two finite simple groups of the same order then they are isomorphic except for the pairs

$$(\mathrm{PSL}_4(\mathbb{F}_2), \mathrm{PSL}_3(\mathbb{F}_4)) \text{ and } (\mathrm{PSO}_{2n+1}(\mathbb{F}_q), \mathrm{PSp}_{2n}(\mathbb{F}_q)) \text{ for } n \geq 3, q \text{ odd.}$$

Artin proved this result for the finite simple groups that were known then. As new finite simple groups were discovered, Tits ([41, 42, 43, 46, 47, 48]) verified that the above examples are the only examples of order coincidence. One may also look in [23] for an exposition of these proofs.

The aim of this chapter is to investigate the situation for the finite semisimple groups. A *finite semisimple group* is defined to be the group of \mathbb{F}_q -rational points of a simply connected, split, semisimple algebraic group defined over \mathbb{F}_q . By lemma (II.10), the orders of the groups $H(\mathbb{F}_q)$ and $H'(\mathbb{F}_q)$ are the same if H and H' are isogenous, and since the simply connected group is unique in an isogeny class, we concentrate only on the simply connected groups. It is easy to see by simple examples that the order of $H(\mathbb{F}_q)$, for a semisimple simply connected algebraic group H defined over \mathbb{F}_q , does not determine the group H . Then one wonders if all examples of the order coincidence in finite semisimple groups can be explicitly described. We prove that it can be done under some mild conditions. We feel that our list of examples of order coincidence in finite semisimple groups is complete, i.e., the mild conditions can be removed, but we have not been to prove it. We also give a geometric reasoning for the order coincidence.

Fix a finite field \mathbb{F}_q and let H be a simply connected, split, semisimple algebraic group defined over \mathbb{F}_q . Let W be the Weyl group of H and let d_1, \dots, d_m

be the fundamental degrees of W counted with multiplicities. Let N denote half the number of the roots of H . Then the order of the finite group $H(\mathbb{F}_q)$ is given by the following formula:

$$|H(\mathbb{F}_q)| = q^N (q^{d_1} - 1)(q^{d_2} - 1) \cdots (q^{d_m} - 1).$$

We now compute the orders of $H(\mathbb{F}_q)$ for all split, simple, simply connected \mathbb{F}_q -groups. We refer to tables 1 and 2 for the information regarding the order of $\Phi(H)$ and the fundamental degrees of $W(H)$.

$$\begin{aligned} |A_n(\mathbb{F}_q)| &= q^{n(n+1)/2} (q^2 - 1)(q^3 - 1) \cdots (q^{n+1} - 1), & n \geq 1, \\ |B_n(\mathbb{F}_q)| &= q^{n^2} (q^2 - 1)(q^4 - 1) \cdots (q^{2n} - 1), & n \geq 2, \\ |C_n(\mathbb{F}_q)| &= q^{n^2} (q^2 - 1)(q^4 - 1) \cdots (q^{2n} - 1), & n \geq 3, \\ |D_n(\mathbb{F}_q)| &= q^{n(n-1)} (q^2 - 1)(q^4 - 1) \cdots (q^{2n-2} - 1)(q^n - 1), & n \geq 4, \\ |G_2(\mathbb{F}_q)| &= q^6 (q^2 - 1)(q^6 - 1), \\ |F_4(\mathbb{F}_q)| &= q^{24} (q^2 - 1)(q^6 - 1)(q^8 - 1)(q^{12} - 1), \\ |E_6(\mathbb{F}_q)| &= q^{36} (q^2 - 1)(q^5 - 1)(q^6 - 1)(q^8 - 1)(q^9 - 1)(q^{12} - 1), \\ |E_7(\mathbb{F}_q)| &= q^{63} (q^2 - 1)(q^6 - 1)(q^8 - 1)(q^{10} - 1)(q^{12} - 1)(q^{14} - 1)(q^{18} - 1), \\ |E_8(\mathbb{F}_q)| &= q^{120} (q^2 - 1)(q^8 - 1)(q^{12} - 1)(q^{14} - 1)(q^{18} - 1)(q^{20} - 1) \\ &\quad (q^{24} - 1)(q^{30} - 1). \end{aligned}$$

The order of the group $C_n(\mathbb{F}_q)$ is the same as that of $B_n(\mathbb{F}_q)$ for all $n \geq 3$ and for all q , so we do not distinguish between these groups in this chapter. Note that the groups $B_n(\mathbb{F}_q)$ and $C_n(\mathbb{F}_q)$ are isomorphic if and only if q is even ([23, Lemma 2.5]).

§17. Some preliminary lemmas.

Artin in [2, 3] obtained some estimates on the power of a prime that can divide $(q^m - 1)$. We recall these results here.

Let $\phi_n(x)$ be the n -th cyclotomic polynomial and

$$\Phi_n(x, y) = y^{\varphi(n)} \phi_n(x/y)$$

be the corresponding homogeneous form. Let a, b be integers which are relatively prime and which satisfy the inequality

$$|a| \geq |b| + 1 \geq 2.$$

Fix a prime p which divides $a^n - b^n$ for some n . Then it is clear that p does not divide any of a and b . Let f be the order of a/b modulo p . For a natural number m , we put $\text{ord}_p m = \alpha$ where p^α is the largest power of p dividing m . We call $p^{\text{ord}_p m}$ the p -contribution to m . Since $f \mid p - 1$, we have $\text{ord}_p f = 0$.

(IV.1) Lemma (Artin [2, Lemma 1]). *With above notations, we have the following rules:*

(1) *If p is odd:*

$$\text{ord}_p \Phi_f(a, b) > 0, \quad \text{ord}_p \Phi_{fp^i}(a, b) = 1 \text{ for } i \geq 1$$

and in all other cases $\text{ord}_p \Phi_n(a, b) = 0$.

Therefore, we have

$$\text{ord}_p(a^n - b^n) = \begin{cases} 0 & \text{if } f \nmid n, \\ \text{ord}_p(a^f - b^f) + \text{ord}_p n & \text{otherwise.} \end{cases}$$

(2) *If $p = 2$, then $f = 1$:*

(a) *If $\Phi_1(a, b) = a - b \equiv 0 \pmod{4}$, then $\text{ord}_2 \Phi_{2^i}(a, b) = 1$ for $i \geq 1$.*

(b) *If $\Phi_2(a, b) = a + b \equiv 0 \pmod{4}$, then $\text{ord}_2 \Phi_{2^i}(a, b) = 1$ for $i = 0, 2, 3, \dots$*

In all other cases $\text{ord}_2 \Phi_n(a, b) = 0$.

(IV.2) Lemma (Artin [3, page 464]). *Let $\alpha = (a-1)(a^2-1) \cdots (a^l-1)$ for some integer $a \neq 0$ and let p_1 be a prime dividing α . Let P_1 be the p_1 -contribution to α , i.e., let P_1 be the highest power of p_1 dividing α and let q be a prime power. We have:*

(1) *If $a = \pm q$, then $P_1 \leq 2^l(q+1)^l$.*

(2) *If $a = q^2$, then $P_1 \leq 4^l(q+1)^l$.*

(IV.3) Lemma (Artin [2, Corollary to Lemma 2]). *If $a > 1$ is an integer and $n > 2$ then there is a prime p which divides $\phi_n(a)$ but no $\phi_i(a)$ with $i < n$ unless $n = 6$ and $a = 2$.*

The following lemma is easy to prove.

(IV.4) Lemma. *If the inequality $q^n \geq \alpha(q+1)$, where α is a fixed positive real number, holds for a pair of positive integers (q_1, n_1) , then it holds for all (q_2, n_2) satisfying $q_2 \geq q_1$ and $n_2 \geq n_1$.*

§18. Determining the finite field.

The first natural step in determining the field \mathbb{F}_q is to determine its characteristic. Observe that if we have two semisimple groups H_1 and H_2 defined over finite fields $\mathbb{F}_{p_1^{r_1}}$ and $\mathbb{F}_{p_2^{r_2}}$ respectively, such that $|H_1(\mathbb{F}_{p_1^{r_1}})| = |H_2(\mathbb{F}_{p_2^{r_2}})|$ and $p_1 \neq p_2$, then either p_1 fails to give the largest contribution to the order of $H_1(\mathbb{F}_{p_1^{r_1}})$ or p_2 fails to give the largest contribution to the order of $H_2(\mathbb{F}_{p_2^{r_2}})$. Therefore we first obtain the description of the split semisimple algebraic groups H defined over \mathbb{F}_{p^r} such that the p -contribution to the order of the group $H(\mathbb{F}_{p^r})$ is not the largest. These groups are the only possible obstructions for determining the

characteristic of the base field. Since we consider simply connected groups only, every semisimple group considered in this paper is a direct product of (simply connected) simple algebraic groups. Hence we need to describe simple algebraic groups H defined over \mathbb{F}_{p^r} with the property that p does not contribute the largest to the order of $H(\mathbb{F}_{p^r})$. We describe such groups in proposition (IV.5) and then prove that under some mild conditions the characteristic of \mathbb{F}_q can be determined by the order of $H(\mathbb{F}_q)$. Once the characteristic is determined, we prove that the field is determined in theorem (IV.8).

18.A. Determining the characteristic of the finite field. We remark that the main tool in the proof of the following proposition is lemma (IV.1) which is proved by Artin in [2]. Our proof of the following proposition is very much on the lines of Artin's proof of Theorem 1 in [3]. However, our result is for $H(\mathbb{F}_q)$, the groups of \mathbb{F}_q -rational points of a simple algebraic group H defined over \mathbb{F}_q whereas Artin proved the result for finite simple groups. The groups $H(\mathbb{F}_q)$ that we consider here, are not always simple, because of the presence of (finite) center. Therefore, we encounter slightly different groups than Artin did, and so we have to sometime use different methods in our proof. Moreover, our list of groups where the characteristic fails to contribute the largest to the order is different than the list described by Artin in [3, Theorem 1].

(IV.5) Proposition. *Let H be a split simple algebraic group defined over a finite field \mathbb{F}_q of characteristic p . If the p -contribution to the order of the finite group $H(\mathbb{F}_q)$ is not the largest prime power dividing the order, then the group $H(\mathbb{F}_q)$ is:*

- (1) $A_1(\mathbb{F}_q)$ for $q \in \{8, 9, 2^r, p\}$ where $2^r + 1$ is a Fermat prime and p is a prime of the type $2^s \pm 1$ or
- (2) $B_2(\mathbb{F}_3)$.

Moreover in all these cases, the p -contribution is the second largest prime power dividing the order of the group $H(\mathbb{F}_q)$.

Proof: We refer to §16 for the orders of the finite groups $H(\mathbb{F}_q)$ where H is a split simple group defined over \mathbb{F}_q . Now, let H be one of the finite simple \mathbb{F}_q -groups and let p_1 be a prime dividing the order of the finite group $H(\mathbb{F}_q)$ such that $p_1 \nmid q$. We use lemma (IV.2) to estimate P_1 , the p_1 -contribution to the order of $H(\mathbb{F}_q)$. Depending on the type of H , we put the following values of a and l in lemma (IV.2).

H	A_n	B_n, D_n	G_2	F_4	E_6	E_7	E_8
a	q	q^2	q^2	q^2	q	q^2	q^2
l	$n + 1$	n	3	6	12	9	15

Now, suppose that the p -contribution to the order of the group $H(\mathbb{F}_q)$ is not the largest, i.e., the power of q that appears in the formula for $|H(\mathbb{F}_q)|$ is smaller

than P_1 for some prime $p_1 \nmid q$. Then, depending on the type of the group, we get following inequalities from lemma (IV.2):

$$\begin{array}{llll}
A_n : P_1 \leq 2^{n+1}(q+1)^{n+1} & \implies & q^{n/2} < 2(q+1), \\
B_n : P_1 \leq 4^n(q+1)^n & \implies & q^n < 4(q+1), \\
D_n : P_1 \leq 4^n(q+1)^n & \implies & q^{n-1} < 4(q+1), \\
G_2 : P_1 \leq 4^3(q+1)^3 & \implies & q^2 < 4(q+1), \\
F_4 : P_1 \leq 4^6(q+1)^6 & \implies & q^4 < 4(q+1), \\
E_6 : P_1 \leq 2^{12}(q+1)^{12} & \implies & q^3 < 2(q+1), \\
E_7 : P_1 \leq 4^9(q+1)^9 & \implies & q^7 < 4(q+1), \\
E_8 : P_1 \leq 4^{15}(q+1)^{15} & \implies & q^8 < 4(q+1).
\end{array}$$

In all the cases where the above inequalities of the type $q^m < \alpha(q+1)$ do not hold, we get that p contributes the largest to the order of $H(\mathbb{F}_q)$. Observe that the last four inequalities, i.e., the inequalities corresponding to the groups F_4 , E_6 , E_7 and E_8 do not hold for $q = 2$ and hence by lemma (IV.4) they do not hold for any $q \geq 2$. Thus, for $H = F_4, E_6, E_7$ and E_8 , the p -contribution to $|H(\mathbb{F}_q)|$ is always the largest prime power dividing $|H(\mathbb{F}_q)|$.

Similarly we obtain following table of the pairs of positive integers (q, n) where the remaining inequalities fail. Then using lemma (IV.4), we know that for all (q', n') with $q' \geq q$ and $n' \geq n$, the contribution of the characteristic to the order of the finite group $H(\mathbb{F}_q)$ is the largest. Therefore, we are left with the cases for (q', n') such that $q' < q$ or $n' < n$, which are to be checked. The adjoining table shows the groups $H(\mathbb{F}_q)$ which are to be checked.

A_n	$q = 2$	$n \geq 6$	$A_3(\mathbb{F}_2), A_3(\mathbb{F}_3), A_3(\mathbb{F}_4), A_3(\mathbb{F}_5),$
	$q = 3, 4, 5$	$n \geq 4$	$A_4(\mathbb{F}_2), A_5(\mathbb{F}_2),$
	$q \geq 7$	$n \geq 3$	$A_1(\mathbb{F}_q), A_2(\mathbb{F}_q) \quad \forall q,$
B_n	$q = 2$	$n \geq 4$	$B_2(\mathbb{F}_2), B_2(\mathbb{F}_3), B_2(\mathbb{F}_4),$
	$q = 3, 4$	$n \geq 3$	$B_3(\mathbb{F}_2),$
	$q \geq 5$	$n \geq 2$	
D_n	$q = 2$	$n \geq 5$	$D_4(\mathbb{F}_2),$
	$q \geq 3$	$n \geq 4$	
G_2	$q \geq 5$		$G_2(\mathbb{F}_2), G_2(\mathbb{F}_3), G_2(\mathbb{F}_4).$

In all the cases other than $A_1(\mathbb{F}_q)$ and $A_2(\mathbb{F}_q)$, we can do straightforward calculations and check that p contributes the largest to the order of every group except for $B_2(\mathbb{F}_3)$. In the case of $B_2(\mathbb{F}_3)$, since $|B_2(\mathbb{F}_3)| = 2^7 \cdot 3^4 \cdot 5$, the prime 3 indeed fails to give the largest contribution, however it gives the second largest contribution to the order of the group. The cases of A_1 and A_2 over a general finite field \mathbb{F}_q are done in a different way.

We first deal with the case of the group $A_2(\mathbb{F}_q)$. Recall that

$$\begin{aligned} |A_2(\mathbb{F}_q)| &= q^3(q^2 - 1)(q^3 - 1) \\ &= q^3(q^2 + q + 1)(q + 1)(q - 1)^2. \end{aligned}$$

Let $p_1 \nmid q$ be a prime dividing the order of $A_2(\mathbb{F}_q)$ and let P_1 be the contribution of p_1 to $|A_2(\mathbb{F}_q)|$. Let f denote the order of q modulo p_1 . If $f \neq 1, 2$ or 3 , then the p_1 -contribution to $(q^2 - 1)(q^3 - 1)$ is 1. If $f = 3$ then p_1 contributes only to $(q^3 - 1)$, whereas if $f = 2$ then p_1 contributes only to $(q^2 - 1)$. Thus, it is clear that in these cases, i.e., when $f \neq 1$, that the p_1 -contribution to the order of $A_2(\mathbb{F}_q)$ is not more than q^3 .

Now we consider the case when $f = 1$. If $p_1 \neq 2$ or 3 , then by lemma (IV.1), P_1 divides $(q - 1)^2$ which is less than q^3 . Thus we only have to check the cases when $p_1 = 2$ or $p_1 = 3$. If $f = 1$ and $p_1 = 2$ or 3 , then P_1 divides either $3(q - 1)^2$, $2(q - 1)^2$ or $4(q + 1)$. Thus, if q^3 is not the largest prime power dividing $|A_2(\mathbb{F}_q)|$, then $q^3 < P_1$ for some prime $p_1 \neq p$ and hence we have

$$q^3 < 3(q - 1)^2, 2(q - 1)^2 \text{ or } 4(q + 1).$$

Again as above, we observe that none of the above inequalities is satisfied by $q \geq 3$, and then we check that the 2-contribution to the order of $A_2(\mathbb{F}_2)$ is the largest one.

Now, for the group $A_1(\mathbb{F}_q)$, we observe that for any prime $p_1 \nmid q$, the p_1 -contribution to the order of $A_1(\mathbb{F}_q)$ divides $q^2 - 1 = (q + 1)(q - 1)$. We make two cases here.

Case (1), $2 \nmid q$: In this case, both $q + 1$ and $q - 1$ are even. The 2-contribution to one of the numbers $q + 1$ and $q - 1$ is 2, and the other number then must be a power of 2 if q is not the largest prime power dividing $|A_1(\mathbb{F}_q)|$.

If $q + 1$ is a power of 2 then we have $q + 1 = p^r + 1 = 2^s$ where p is the characteristic of the group $A_1(\mathbb{F}_q)$. If r is even, p^r would be a square and hence $s = 1$. If r is odd, then $p + 1$ divides $p^r + 1$ and

$$\frac{p^r + 1}{p + 1} = p^{r-1} - p^{r-2} + \cdots - p + 1$$

is an odd divisor of $p^r + 1 = 2^s$, hence we have $r = 1$ and $q = p = 2^s - 1$, a Mersenne prime.

If $q - 1$ is a power of 2 then we have $q - 1 = p^r - 1 = 2^s$. It is clear that $p - 1$ divides $p^r - 1 = 2^s$ and hence $p = 2^m + 1$ is a Fermat prime. If $r = 1$, then $q = p$. If $r = 2$, then $(p^2 - 1)/(p - 1) = p + 1$ is a power of 2. Thus $p + 1$ and $p - 1$ are both powers of 2, but their difference is 2. Hence $p + 1 = 4$, $p - 1 = 2$, i.e., $p = 3$, $q = 9$ and $s = 3$. If $r > 2$, then by lemma (IV.3), there is a prime divisor of $p^r - 1$ which does not divide $p - 1$, a contradiction.

Case (2), $2 \mid q$: In this case, $q - 1$ and $q + 1$ are both odd and hence they do not have any common prime factor. If q is not the largest prime power dividing $|A_1(\mathbb{F}_q)|$, then the largest prime power dividing $|A_1(\mathbb{F}_q)|$ must be $q + 1$. Let $q = 2^r$ and $P_1 = p_1^s = 2^r + 1$. Here p_1 is odd, and hence by lemma (IV.3), if $s > 2$, there is a prime divisor of $p_1^s - 1$ which does not divide $p_1 - 1$, a contradiction. If $s = 2$, $2^r = p_1^2 - 1$. Then both $p_1 \pm 1$ are powers of two and hence we obtain that $p_1 = 3$ and $q = 2^3 = 8$. If $s = 1$, $p_1 = 2^r + 1$, a Fermat prime.

Thus, we have the result that if the p -contribution to the order of the group $H(\mathbb{F}_{p^r})$, where H is a split simple algebraic group defined over the field \mathbb{F}_{p^r} , is not the largest then the possibilities of $H(\mathbb{F}_{p^r})$ are: $A_1(\mathbb{F}_q)$ where $q \in \{8, 9, 2^r, p\}$ where $2^r + 1$ is a Fermat prime and p is a prime of the type $2^s \pm 1$, or the group $B_2(\mathbb{F}_3)$.

In these cases, it can be checked that the contribution of the characteristic to the order of the group $H(\mathbb{F}_q)$ is the second largest prime power dividing the order. \square

If $H(\mathbb{F}_q)$ is not one of the groups described in the above proposition, then the characteristic of \mathbb{F}_q contributes the largest to the order of $H(\mathbb{F}_q)$. Since every (simply connected) semisimple algebraic group is a direct product of (simply connected) simple algebraic groups, we get that whenever a finite semisimple group $H(\mathbb{F}_q)$ does not have any of the above groups as direct factors, then the characteristic of \mathbb{F}_q contributes the largest to the order of $H(\mathbb{F}_q)$.

(IV.6) Theorem. *Let H_1 and H_2 be two split semisimple simply connected algebraic groups defined over finite fields \mathbb{F}_{q_1} and \mathbb{F}_{q_2} respectively. Let X denote the set $\{8, 9, 2^r, p\}$ where $2^r + 1$ is a Fermat prime and p is a prime of the type $2^s \pm 1$. Suppose that for $i = 1, 2$, A_1 is not one of the direct factors of H_i whenever $q_i \in X$ and B_2 is not a direct factor of H_i whenever $q_i = 3$. Then, if $|H_1(\mathbb{F}_{q_1})| = |H_2(\mathbb{F}_{q_2})|$, the characteristics of \mathbb{F}_{q_1} and \mathbb{F}_{q_2} are the same.*

Proof: Let p_1 and p_2 be the respective characteristics of the fields \mathbb{F}_{q_1} and \mathbb{F}_{q_2} . For $i = 1, 2$ and any integer m , we denote the p_i -contribution to m by $P_i(m)$. Since the groups mentioned in proposition (IV.5) do not occur as direct factors of the semisimple groups H_i , we have

$$P_1(|H_1(\mathbb{F}_{q_1})|) \geq P_2(|H_1(\mathbb{F}_{q_1})|) \quad \text{and} \quad P_2(|H_2(\mathbb{F}_{q_2})|) \geq P_1(|H_2(\mathbb{F}_{q_2})|).$$

Since $|H_1(\mathbb{F}_{q_1})| = |H_2(\mathbb{F}_{q_2})|$, we have

$$P_1(|H_1(\mathbb{F}_{q_1})|) = P_1(|H_2(\mathbb{F}_{q_2})|) \quad \text{and} \quad P_2(|H_1(\mathbb{F}_{q_1})|) = P_2(|H_2(\mathbb{F}_{q_2})|).$$

This gives us that $P_1(|H_1(\mathbb{F}_{q_1})|) = P_2(|H_1(\mathbb{F}_{q_1})|)$. Since P_1 and P_2 are powers of the primes p_1 and p_2 respectively, this implies that $p_1 = p_2$. \square

(IV.7) Remark. Since $|A_1(\mathbb{F}_9)| = |B_2(\mathbb{F}_2)|$, the above theorem is not true in general. We feel that this is the only counter example, i.e., the conclusion of the theorem (IV.6) is true without the hypothesis imposed there except that we must exclude the case of $H_1 = A_1$ over \mathbb{F}_9 and $H_2 = B_2$ over \mathbb{F}_2 , but we have not been able to prove it.

18.B. Determining the finite field. Now, we come to the main result of this section. Recall that if H is a split semisimple algebraic group of rank n defined over a finite field \mathbb{F}_q , then the order of $H(\mathbb{F}_q)$ is given by the formula,

$$|H(\mathbb{F}_q)| = q^N (q^{d_1} - 1)(q^{d_2} - 1) \cdots (q^{d_m} - 1)$$

where d_1, d_2, \dots, d_m are the fundamental degrees of $W(H)$, the Weyl group of H and N is half the number of the roots of H . Incidentally, we also have

$$N = \sum_i (d_i - 1).$$

(IV.8) Theorem. Let H_1 and H_2 be two split semisimple simply connected algebraic groups defined over finite fields \mathbb{F}_{q_1} and \mathbb{F}_{q_2} of the same characteristic. Suppose that the order of the finite groups $H_1(\mathbb{F}_{q_1})$ and $H_2(\mathbb{F}_{q_2})$ are the same, then $q_1 = q_2$. Moreover the fundamental degrees (and the multiplicities) of the Weyl groups $W(H_1)$ and $W(H_2)$ are the same.

Proof: Let p be the characteristic of the fields \mathbb{F}_{q_1} and \mathbb{F}_{q_2} , and let $q_1 = p^{t_1}, q_2 = p^{t_2}$. Let the orders of the finite groups $H_1(\mathbb{F}_{q_1})$ and $H_2(\mathbb{F}_{q_2})$ be given by,

$$\begin{aligned} |H_1(\mathbb{F}_{q_1})| &= (q_1)^r (q_1^{r_1} - 1)(q_1^{r_2} - 1) \cdots (q_1^{r_n} - 1) \\ &= (p^{t_1})^r ((p^{t_1})^{r_1} - 1)((p^{t_1})^{r_2} - 1) \cdots ((p^{t_1})^{r_n} - 1) \\ |H_2(\mathbb{F}_{q_2})| &= (q_2)^s (q_2^{s_1} - 1)(q_2^{s_2} - 1) \cdots (q_2^{s_m} - 1) \\ &= (p^{t_2})^s ((p^{t_2})^{s_1} - 1)((p^{t_2})^{s_2} - 1) \cdots ((p^{t_2})^{s_m} - 1) \end{aligned}$$

As remarked above, the integers r_i and s_j are the respective fundamental degrees of the Weyl groups $W(H_1)$ and $W(H_2)$. Moreover the rank of the group H_1 is n and that of H_2 is m . Further, we have

$$r = \sum_{i=1}^n (r_i - 1) \quad \text{and} \quad s = \sum_{j=1}^m (s_j - 1).$$

Since $|H_1(\mathbb{F}_{q_1})| = |H_2(\mathbb{F}_{q_2})|$, we have that

$$t_1 r = t_2 s$$

and

$$(9) \quad \prod_{i=1}^n ((p^{t_1})^{r_i} - 1) = \prod_{j=1}^m ((p^{t_2})^{s_j} - 1).$$

Assume that $r_1 \leq r_2 \leq \cdots \leq r_n$ and $s_1 \leq s_2 \leq \cdots \leq s_m$. We treat both the products in the equation (9) as polynomials in p and factor them into the cyclotomic polynomials in p .

Let us assume for the time being that $p \neq 2$, so that we can apply lemma (IV.3) to conclude that the cyclotomic polynomials appearing on both the sides of the equation (9) are the same with the same multiplicities. Observe that on the left hand side (LHS) the highest order cyclotomic polynomial is $\phi_{t_1 r_n}(p)$ whereas such a polynomial on the right hand side (RHS) is $\phi_{t_2 s_m}(p)$. Since the cyclotomic polynomials appearing on both the sides are the same, we have that $t_1 r_n = t_2 s_m$. Thus, the polynomial $p^{t_1 r_n} - 1$, which is the same as the polynomial $p^{t_2 s_m} - 1$, can be canceled from both the sides of the equation (9). Continuing in this way we get that $t_1 r_{n-k} = t_2 s_{m-k}$ for all k . This implies in particular that $m = n$. Further

$$t_1 r = t_2 s \implies \sum_i t_1 (r_i - n) = \sum_j t_2 (s_j - n).$$

But, by above observation, this gives us that $t_1 n = t_2 n$ and hence $t_1 = t_2$, i.e., $q_1 = q_2$. Thus, the fields \mathbb{F}_{q_1} and \mathbb{F}_{q_2} are isomorphic.

Now, it also follows that $r_i = s_i$ for all i , i.e., the fundamental degrees of the corresponding Weyl groups are the same.

Now, let $p = 2$. So, we have the equation

$$(10) \quad (2^{t_1})^r \prod_{i=1}^n ((2^{t_1})^{r_i} - 1) = (2^{t_2})^s \prod_{j=1}^m ((2^{t_2})^{s_j} - 1).$$

The only possible obstruction to the desired result in this case comes from the equations

$$\phi_6(2) = 2^2 - 2 + 1 = 3 \quad \text{and} \quad \phi_2(2) = 2 + 1 = 3.$$

So, we can assume that the cyclotomic polynomials of order $l \neq 1, 2, 3, 6$ occur on both the sides of above equation with the same multiplicities.

Let now $\phi_6(2)$ divide the LHS of the equation and assume that it does not divide the RHS. Since the polynomial $\phi_6(2)$ divides the LHS, the polynomial $2^6 - 1$ appears on the LHS. Since $\phi_6(2)$ does not divide the RHS the prime factors of $2^6 - 1 = 3^2 \cdot 7$ must be adjusted by the polynomial $(2^3 - 1)(2^2 - 1)^2$ in the RHS, i.e., in the formula for $|H_2(\mathbb{F}_{2^{t_2}})|$. Thus, a power of $(2^6 - 1)$ in the LHS and the same power of $(2^3 - 1)(2^2 - 1)^2$ is the only obstruction. Other than these polynomials, all the factors of type $2^l - 1$ occur in both the sides with the same multiplicities.

Being a fundamental degree of a Weyl group, $s_1 > 1$, so $t_2 = 1$, $q_2 = 2$. Similarly since t_1 divides 6, the possible values for q_1 are 2, 2^2 and 2^3 . We make three cases depending on q_1 .

Case (1). If $q_1 = 2$, the equation (10) becomes

$$2^r \prod_{i=1}^n (2^{r_i} - 1) = 2^s \prod_{j=1}^m (2^{s_j} - 1).$$

But then $r = s$ and hence $\sum_i (r_i - 1) = \sum_j (s_j - 1)$. Now, the term $(2^6 - 1)$ contributes 5 to r whereas the term $(2^3 - 1)(2^2 - 1)^2$ contributes only 4 to s . As other factors are the same on both the sides, this is a contradiction. Hence the factor $(2^6 - 1)$ in LHS of the equation (10) must be adjusted by the same factor in the RHS. Then we get that $m = n$ and $r_i = s_i$ for all i .

Case (2). If $q_1 = 2^2$, the equation (10) becomes

$$4^r \prod_{i=1}^n (4^{r_i} - 1) = 2^s \prod_{j=1}^m (2^{s_j} - 1).$$

Then, we get that $2r = s$ and hence $\sum_i 2(r_i - 1) = \sum_j (s_j - 1)$. Now, the term $(2^6 - 1) = (4^3 - 1)$ contributes 2 to r , i.e., 4 to $2r$ and the term $(2^3 - 1)(2^2 - 1)^2$ contributes 4 to s . Since, other factors of type $2^k - 1$ are the same on both sides, the contribution of each $s_j = 2r_{i_j}$ is $2r_{i_j} - 1$ to s whereas r_i contributes $2r_i - 2$ to $2r$. This is a contradiction, unless there are no other factors. But since 2 is always a fundamental degree for $W(H)$ for any split simple group H , we have $(4^2 - 1)$ in the LHS. Thus, we again get that the factor $2^6 - 1$ is adjusted by the same factor in the RHS also.

Case (3). If $q_1 = 2^3$, the equation (10) becomes

$$8^r \prod_{i=1}^n (8^{r_i} - 1) = 2^s \prod_{j=1}^m (2^{s_j} - 1).$$

As above we have $3r = s$ and therefore $\sum_i 3(r_i - 1) = \sum_j (s_j - 1)$. Now, the term $(2^6 - 1) = (8^2 - 1)$ contributes 1 to r , i.e., 3 to $3r$, whereas the term $(2^3 - 1)(2^2 - 1)^2$ contributes 4 to s . Since, other factors of type $2^k - 1$ are the same on both sides, the contribution of each $s_j = 3r_{i_j}$ is $3r_{i_j} - 1$ to s whereas r_i contributes $3r_i - 3$ to $3r$. Thus $3r < s$ and this is a contradiction. Hence the factors $\phi_n(2)$ must be the same on both the sides of the equation (10).

This completes the proof. \square

(IV.9) Theorem. *Let H_1 and H_2 be two split semisimple simply connected algebraic groups defined over a finite field \mathbb{F}_q . If the orders of the finite groups $H_1(\mathbb{F}_q)$ and $H_2(\mathbb{F}_q)$ are the same then the orders of $H_1(\mathbb{F}_{q'})$ and $H_2(\mathbb{F}_{q'})$ are the same for any finite extension $\mathbb{F}_{q'}$ of \mathbb{F}_q .*

Proof: Let H_1, H_2 be split semisimple algebraic groups defined over \mathbb{F}_q . By theorem (IV.8), we have that if $|H_1(\mathbb{F}_q)| = |H_2(\mathbb{F}_q)|$ then the fundamental degrees

of the Weyl groups $W(H_1)$ and $W(H_2)$ are the same with the same multiplicities. Then the formulae for the orders of the groups $H_1(\mathbb{F}_q)$ and $H_2(\mathbb{F}_q)$ are the same as polynomials in q . Hence the orders of the groups $H_1(\mathbb{F}_{q'})$ and $H_2(\mathbb{F}_{q'})$ are the same for any finite extension $\mathbb{F}_{q'}$ of \mathbb{F}_q . \square

§19. Pairs of order coincidence.

We fix a finite field \mathbb{F}_q and all the algebraic groups considered in this section are assumed to be defined over \mathbb{F}_q . In this section, we concentrate on the pairs of order coincidence. We define a *pair of order coincidence* to be a pair of split semisimple groups (H_1, H_2) , such that the orders of the groups $H_1(\mathbb{F}_q)$ and $H_2(\mathbb{F}_q)$ are the same. We want to understand the reason behind the coincidence of these orders and to characterize all possible pairs of order coincidence (H_1, H_2) . We know by theorem (IV.8), that for such a pair (H_1, H_2) , the fundamental degrees of the corresponding Weyl groups, $W(H_1)$ and $W(H_2)$, must be the same with the same multiplicities. We now make following easy observations which follow from the basic theory of the Weyl groups ([19]).

(IV.10) Remark. *Let H_1 and H_2 be two split semisimple simply connected algebraic groups over a finite field \mathbb{F}_q such that the groups $H_1(\mathbb{F}_q)$ and $H_2(\mathbb{F}_q)$ have the same order. Then we have:*

- (1) *The rank of the group H_1 is the same as the rank of H_2 .*
- (2) *The number of direct simple factors of the groups H_1 and H_2 is the same.*
- (3) *If one of the groups, say H_1 , is simple, then so is H_2 and either H_1 is isomorphic to H_2 .*

(We remind the reader once again that we do not distinguish between the groups of type B_n and C_n .)

Next natural step would be to look at the pairs of order coincidence in the case of groups each having two simple factors. We characterize such pairs in the following theorem. For a Weyl group W , we denote the collection of fundamental degrees of W by $d(W)$.

(IV.11) Theorem. *Let H_1 and H_2 be split semisimple simply connected algebraic groups each being a direct product of exactly two simple algebraic groups. Assume that H_1 and H_2 do not have any common simple direct factor. Then the pairs (H_1, H_2) such that $|H_1(\mathbb{F}_q)| = |H_2(\mathbb{F}_q)|$ are exhausted by the following list:*

- (1) $(A_{2n-2}B_n, A_{2n-1}B_{n-1})$ for $n \geq 2$, with the convention that $B_1 = A_1$,
- (2) $(A_{n-2}D_n, A_{n-1}B_{n-1})$ for $n \geq 4$,
- (3) $(B_{n-1}D_{2n}, B_{2n-1}B_n)$ for $n \geq 2$, with the convention that $B_1 = A_1$,
- (4) (A_1A_5, A_4G_2) ,
- (5) (A_1B_3, B_2G_2) ,

- (6) $(A_1 D_6, B_5 G_2)$,
- (7) $(A_2 B_3, A_3 G_2)$ and
- (8) $(B_3^2, D_4 G_2)$.

Proof: Let $H_1 = H_{1,1} \times H_{1,2}$ and $H_2 = H_{2,1} \times H_{2,2}$ where $H_{i,j}$ are split simple algebraic groups. We denote $W(H_i)$ by W_i and $W(H_{i,j})$ by $W_{i,j}$.

Since the orders of the groups $|H_1(\mathbb{F}_q)|$ and $|H_2(\mathbb{F}_q)|$ are the same, by theorem (IV.8), the fundamental degrees of the Weyl groups W_1 and W_2 are the same with the same multiplicities. Moreover for $i = 1, 2$, we have $W_i = W_{i,1} \times W_{i,2}$.

The general philosophy of the method is as follows. Let the largest fundamental degree of $W_{i,1}$ be greater than or equal to the largest fundamental degree of $W_{i,2}$. Once we fix a positive integer n to be the largest fundamental degree of W_1 (which is the same as the largest fundamental degree of W_2), we have a finite set of choices for $H_{1,1}$ and $H_{2,1}$. Then we fix one choice each for $H_{1,1}$ and $H_{2,1}$, and compare the fundamental degrees of $W_{1,1}$ and $W_{2,1}$. Since $H_{1,1} \neq H_{2,1}$ the collections $d(W_{1,1})$ and $d(W_{2,1})$ are different. The fundamental degrees of $W_{1,1}$ that do not occur in $d(W_{2,1})$ must occur in the collection $d(W_{2,2})$ and similarly the fundamental degrees of $W_{2,1}$ that do not occur in $d(W_{1,1})$ must occur in the collection $d(W_{1,2})$. Moreover the fundamental degrees of $W_{1,2}$ and $W_{2,2}$ are bounded above by n . This gives us further finitely many choices for the groups $H_{1,2}$ and $H_{2,2}$. Then we simply verify the equality of the collections $d(W_1)$ and $d(W_2)$. If the collections are equal, we get a coincidence of orders (H_1, H_2) .

Let n be the maximum of the fundamental degrees of W_1 . Suppose that n is the maximum fundamental degree of $W_{1,1}$. Then depending on n , we have following choices for the group $H_{1,1}$:

$n = 4$	$A_3, B_2.$
$n = 6$	$A_5, B_3, D_4, G_2.$
$n = 12$	$A_{11}, B_6, D_7, F_4, E_6.$
$n = 18$	$A_{17}, B_9, D_{10}, E_7.$
$n = 30$	$A_{29}, B_{15}, D_{16}, E_8.$
$n = 2$ or n odd	$A_{n-1}.$
$n = 2m, m \notin \{1, 2, 3, 6, 9, 15\}$	$A_{2m-1}, B_m, D_{m+1}.$

Let $n = 4$. Let us assume that $H_{1,1} = A_3$. Since the groups H_1 and H_2 do not have any common simple direct factor, A_3 is not a factor of H_2 . Therefore, one of the $H_{2,j}$, say $H_{2,1}$ is B_2 . Then we have

$$d(W_{1,1}) = \{2, 3, 4\} \quad \text{and} \quad d(W_{2,1}) = \{2, 4\}.$$

Thus, 3 is a fundamental degree of $W_{2,2}$ and the maximum of the fundamental degrees of $W_{2,2}$ is less than or equal to 4, hence $H_{2,2} = A_2$. Then, since $d(W_1) = d(W_2)$, the only possibility for the collection $d(W_{1,2})$ is $\{2\}$ and we get that

$H_{1,2} = A_2$. This gives us the order coincidence

$$(A_1A_3, A_2B_2).$$

Let $n = 6$. We make several cases depending on the choice of $H_{1,1}$.

Case (1): Let $H_{1,1} = G_2$. Since H_1 and H_2 do not have any common direct simple factor, G_2 is not a direct factor of H_2 . Then one of the factors of H_2 , say $H_{2,1}$ is one of the groups A_5, B_3 and D_4 .

Suppose $H_{2,1} = D_4$. Then we have

$$d(W_{1,1}) = \{2, 6\} \quad \text{and} \quad d(W_{2,1}) = \{2, 4, 4, 6\}.$$

Since the collections $d(W_1)$ and $d(W_2)$ are the same, we have that $\{4, 4\}$ must be a subcollection of $d(W_{1,2})$. But then $H_{1,2} = D_4$ since the collection $d(W_{1,2})$ is bounded above by 6. But this is a contradiction, as H_1 and H_2 do not have any common simple direct factor.

Suppose $H_{2,1} = B_3$. Then we have

$$d(W_{1,1}) = \{2, 6\} \quad \text{and} \quad d(W_{2,1}) = \{2, 4, 6\}.$$

Therefore $4 \in d(W_{1,2})$ and the collection $d(W_{1,2}) - \{4\}$ is also a valid collection of fundamental degrees, in fact, it is the collection $d(W_{2,2})$. Moreover the maximum of the collection $d(W_{1,2})$ is less than or equal to 6. This gives us the possible choices for $H_{1,2}$ as D_4, B_2, A_3 and the corresponding pairs of order coincidence are

$$(G_2D_4, B_3^2), (G_2B_2, B_3A_1) \quad \text{and} \quad (G_2A_3, B_3A_2).$$

Finally suppose $H_{2,1} = A_5$. Then we have

$$d(W_{1,1}) = \{2, 6\} \quad \text{and} \quad d(W_{2,1}) = \{2, 3, 4, 5, 6\}.$$

Therefore $\{3, 4, 5\}$ is a subcollection of $d(W_{1,2})$, thus implying that $H_{1,2} = A_4$ since the maximum of fundamental degrees of $W_{1,2}$ is less than or equal to 6. This gives us another order coincidence

$$(G_2A_4, A_5A_1).$$

Case (2): Now we let $H_{1,1} = D_4$. We can assume that G_2 is not one of the simple factors of H_2 , thanks to the case above, therefore we have B_3 and A_5 as the only possible choices for $H_{2,1}$.

Suppose $H_{2,1} = A_5$. Then we have

$$d(W_{1,1}) = \{2, 4, 4, 6\} \quad \text{and} \quad d(W_{2,1}) = \{2, 3, 4, 5, 6\}.$$

Then $5 \in d(W_{1,2})$ and therefore $4 \in d(W_{1,2})$. Thus, we have that 4 occurs with multiplicity 3 in $d(W_1) = d(W_2)$. Since the multiplicity of 4 in $d(W_{2,1})$ is 1, the same in $d(W_{2,2})$ is 2. But then $H_{2,2}$ is D_4 , since the set $d(W_2)$ is bounded above by 6. This is a contradiction since H_1 and H_2 do not have any common factor.

Suppose $H_{2,1} = B_3$. Then we have

$$d(W_{1,1}) = \{2, 4, 4, 6\} \quad \text{and} \quad d(W_{2,1}) = \{2, 4, 6\}.$$

Therefore $4 \in d(W_{2,2})$ such that $d(W_{2,2}) - \{4\} = d(W_{1,2})$. This gives us possible choices of $H_{2,2}$ as B_2, A_3 and we get following pairs of order coincidence:

$$(D_4A_1, B_3B_2) \quad \text{and} \quad (D_4A_2, B_3A_3).$$

Case (3): Finally we let $H_{1,1} = B_3$. We now assume that G_2 and D_4 do not appear as factors, therefore $H_{2,1} = A_5$. Then we have

$$d(W_{1,1}) = \{2, 4, 6\} \quad \text{and} \quad d(W_{2,1}) = \{2, 3, 4, 5, 6\}.$$

Therefore $\{3, 5\} \subseteq d(W_{1,2})$ and $d(W_{1,2}) - \{3, 5\} = d(W_{2,2})$. This implies that $H_{1,2} = A_4$ and $H_{2,2} = B_2$, and the order coincidence we get is

$$(B_3A_4, A_5B_2).$$

This completes the case for $n = 6$.

We follow the same method for other cases and get the required result. \square

Observe that in the above theorem, we have three infinite families of pairs,

$$(A_{2n-2}B_n, A_{2n-1}B_{n-1}), (A_{n-2}D_n, A_{n-1}B_{n-1}) \quad \text{and} \quad (B_{n-1}D_{2n}, B_{2n-1}B_n).$$

If we consider the following pairs given by the first two infinite families:

$$(H_1, H_2) = (A_{2n-2}B_n, A_{2n-1}B_{n-1}) \quad \text{and} \quad (H_3, H_4) = (A_{2n-2}D_{2n}, A_{2n-1}B_{2n-1})$$

then

$$(H_1H_4, H_2H_3) = (A_{2n-2}A_{2n-1}B_nB_{2n-1}, A_{2n-1}A_{2n-2}B_{n-1}D_{2n}).$$

This implies that $(B_{2n-1}B_n, B_{n-1}D_{2n})$ is also a pair of order coincidence and this is precisely our third infinite family! Thus, the third infinite family of pairs of order coincidence can be obtained from the first two infinite families.

Similarly if we consider

$$(H_1, H_2) = (A_2D_4, A_3B_3) \quad \text{and} \quad (H_3, H_4) = (A_2B_3, A_3G_2),$$

then we get the pair (B_3^2, D_4G_2) from the pair (H_2H_3, H_1H_4) .

Similarly we observe that

$$\begin{aligned} (A_1B_3, B_2G_2) &\text{ can be obtained from } (A_1A_3, A_2B_2) \text{ and } (A_2B_3, A_3G_2), \\ (A_1A_5, A_4G_2) &\text{ can be obtained from } (A_4B_3, A_5B_2) \text{ and } (A_1B_3, B_2G_2), \\ (A_1D_6, B_5G_2) &\text{ can be obtained from } (A_4D_6, A_5B_5) \text{ and } (A_1A_5, A_4G_2). \end{aligned}$$

We record our observation as a remark below.

(IV.12) Remark. *All pairs of order coincidence described in theorem (IV.11) can be obtained from the following pairs:*

$$(1) \quad (A_{2n-2}B_n, A_{2n-1}B_{n-1}) \text{ for } n \geq 2, \text{ with the convention that } B_1 = A_1,$$

- (2) $(A_{n-2}D_n, A_{n-1}B_{n-1})$ for $n \geq 4$, and
- (3) (A_2B_3, A_3G_2) .

These pairs are quite special, in the sense that they admit a geometric reasoning for the coincidence of orders. We describe it in the last section, §21.

If we do not restrict ourselves to the groups having exactly two simple factors, then we also find the following pairs (H_1, H_2) involving other exceptional groups:

$$(A_1B_4B_6, B_2B_5F_4), (A_4G_2A_8B_6, A_3A_6B_5E_6), (A_1B_7B_9, B_2B_8E_7),$$

$$\text{and } (A_1B_4B_7B_{10}B_{12}B_{15}, B_3B_5B_8B_{11}B_{14}E_8).$$

One now asks a natural question whether these four pairs, together with the pairs described in the remark (IV.12), generate all possible pairs of order coincidence. We make this question more precise in the next section and answer it in the affirmative.

§20. On a group structure on pairs of order coincidence.

Fix a finite field \mathbb{F}_q . Let \mathcal{A} be the set of ordered pairs (H_1, H_2) of order coincidence of split semisimple algebraic groups defined over the field \mathbb{F}_q . We define an equivalence relation on \mathcal{A} by saying that an element $(H_1, H_2) \in \mathcal{A}$ is related to $(H'_1, H'_2) \in \mathcal{A}$, denoted by $(H_1, H_2) \sim (H'_1, H'_2)$, if and only if there exist two split semisimple algebraic groups H and K defined over \mathbb{F}_q such that

$$H'_1 \times K = H_1 \times H \quad \text{and} \quad H'_2 \times K = H_2 \times H.$$

It can be checked that \sim is an equivalence relation. We denote the set of equivalence classes, \mathcal{A}/\sim , by \mathcal{G} and the equivalence class of an element $(H_1, H_2) \in \mathcal{A}$ is denoted by $[(H_1, H_2)]$. This set \mathcal{G} describes all pairs of order coincidence (H_1, H_2) where the split semisimple (simply connected) groups H_i do not have any common direct simple factor.

We put a binary operation on \mathcal{G} given by

$$[(H_1, H_2)] \circ [(H'_1, H'_2)] = [(H_1 \times H'_1, H_2 \times H'_2)].$$

It is easy to see that the above operation is well defined modulo the equivalence that we have introduced. The set \mathcal{G} is obviously closed under \circ which is an associative operation. The equivalence class $[(H, H)]$ acts as the identity and $[(H_1, H_2)]^{-1} = [(H_2, H_1)]$. Thus \mathcal{G} is an abelian torsion-free group. Since the first two infinite families described in the remark (IV.12) are independent, the group \mathcal{G} is not finitely generated.

Let \mathcal{G}' be the subgroup of \mathcal{G} generated by following elements.

- (1) $B_n = [(A_{2n-2}B_n, A_{2n-1}B_{n-1})]$ for $n \geq 2$, with the convention that $B_1 = A_1$,
- (2) $D_n = [(A_{n-2}D_n, A_{n-1}B_{n-1})]$ for $n \geq 4$,

- (3) $G_2 = [(A_2B_3, A_3G_2)]$,
- (4) $F_4 = [(A_1B_4B_6, B_2B_5F_4)]$,
- (5) $E_6 = [(A_4G_2A_8B_6, A_3A_6B_5E_6)]$,
- (6) $E_7 = [(A_1B_7B_9, B_2B_8E_7)]$,
- (7) $E_8 = [(A_1B_4B_7B_{10}B_{12}B_{15}, B_3B_5B_8B_{11}B_{14}E_8)]$.

(For a group such as B_n , we use B_n to denote a pair (H_1, H_2) in which B_n appears with the largest fundamental degree.)

(IV.13) Lemma. *Let n be a positive integer. Let H_1 and H_2 be split, simply connected, simple algebraic groups such that the Weyl groups $W(H_1)$ and $W(H_2)$ have the same highest fundamental degree and it is equal to n . Then there is an element in \mathcal{G}' which can be represented as the equivalence class of a pair (K_1, K_2) of order coincidence such that for $i = 1, 2$, H_i is one of the simple factors of K_i and for any other simple factor H'_i of K_i the highest fundamental degree of $W(H'_i)$ is less than n .*

Proof: We prove this lemma by explicit calculations. If n is odd or $n = 2$, there is nothing to prove as there is only one group, A_{n-1} , with n as the highest fundamental degree. Further, the groups A_3 and B_2 are the only groups with 4 as the highest fundamental degree and $B_2 = [(A_2B_2, A_3B_1)]$ is an element of the group \mathcal{G}' where A_3 and B_2 appear as factors on either sides and all other simple groups that appear have highest fundamental degree less than 4.

If $n = 2m$ for $m > 2$ and $m \notin \{3, 6, 9, 15\}$, then A_{2m-1} , B_m and D_{m+1} are the only groups with n as the highest fundamental degree. Consider following elements of \mathcal{G}' :

$$B_m = [(A_{2m-2}B_m, A_{2m-1}B_{m-1})], \quad D_{m+1} = [(A_{m-1}D_{m+1}, A_mB_m)]$$

$$\text{and } D_{m+1} \circ B_m = [(A_{m-1}A_{2m-2}D_{m+1}, A_mA_{2m-1}B_{m-1})].$$

The element B_m contains the simple groups A_{2m-1} and B_m on its either sides and other simple groups appearing in B_m have highest fundamental degree less than $2m$. Similarly the elements D_{m+1} and $D_{m+1}B_m$ are the required elements of \mathcal{G}' for the pairs $\{D_{m+1}, B_m\}$ and $\{A_{2m-1}, D_{m+1}\}$.

Now, we consider the cases when $n = 6, 12, 18, 30$. These cases involve exceptional groups. We have following elements of \mathcal{G}' for the corresponding pairs:

$$\begin{array}{ll} B_3 = [(A_4B_3, A_5B_2)] & \text{for the pair } \{B_3, A_5\}, \\ D_4 = [(A_2D_4, A_3B_3)] & \text{for the pair } \{D_4, B_3\}, \\ G_2 = [(A_2B_3, A_3G_2)] & \text{for the pair } \{B_3, G_2\}, \\ D_4 \circ G_2 = [(A_2^2D_4, A_3^2G_2)] & \text{for the pair } \{D_4, G_2\}, \\ B_3 \circ D_4 = [(A_2A_4D_4, A_3A_5B_2)] & \text{for the pair } \{D_4, A_5\}, \\ G_2 \circ B_3^{-1} = [(A_2A_5B_2, A_3A_4G_2)] & \text{for the pair } \{A_5, G_2\}. \end{array}$$

In the same way, we give following elements of the group \mathcal{G}' for all possible simple groups having highest fundamental degree 12, 18 and 30.

$n = 12$

pair	element of \mathcal{G}'
$\{B_6, D_7\}$	$D_7 = [(A_5 D_7, A_6 B_6)]$
$\{B_6, A_{11}\}$	$B_6 = [(A_{10} B_6, A_{11} B_5)]$
$\{B_6, F_4\}$	$F_4 = [(A_1 B_4 B_6, B_2 B_5 F_4)]$
$\{B_6, E_6\}$	$E_6 = [(A_4 G_2 A_8 B_6, A_3 A_6 B_5 E_6)]$
$\{D_7, A_{11}\}$	$B_6 \circ D_7$
$\{D_7, F_4\}$	$D_7 \circ F_4$
$\{D_7, E_6\}$	$D_7 \circ E_6$
$\{A_{11}, F_4\}$	$B_6^{-1} \circ F_4$
$\{A_{11}, E_6\}$	$B_6^{-1} \circ E_6$
$\{F_4, E_6\}$	$F_4^{-1} \circ E_6$

$n = 18$

pair	element of \mathcal{G}'
$\{B_9, D_{10}\}$	$D_{10} = [(A_8 D_{10}, A_9 B_9)]$
$\{B_9, A_{17}\}$	$B_9 = [(A_{16} B_9, A_{17} B_8)]$
$\{B_9, E_7\}$	$E_7 = [(A_1 B_7 B_9, B_2 B_8 E_7)]$
$\{D_{10}, A_{17}\}$	$B_9 \circ D_{10}$
$\{D_{10}, E_7\}$	$D_{10} \circ E_7$
$\{A_{17}, E_7\}$	$B_9^{-1} \circ E_7$

$n = 30$

pair	element of \mathcal{G}'
$\{B_{15}, A_{29}\}$	$B_{15} = [(A_{28} B_{15}, A_{29} B_{14})]$
$\{B_{15}, D_{16}\}$	$D_{16} = [(A_{14} D_{16}, A_{15} B_{15})]$
$\{B_{15}, E_8\}$	$E_8 = [(A_1 B_4 B_7 B_{10} B_{12} B_{15}, B_3 B_5 B_8 B_{11} B_{14} E_8)]$
$\{D_{16}, A_{29}\}$	$B_{15} \circ D_{16}$
$\{D_{16}, E_8\}$	$D_{16} \circ E_8$
$\{A_{29}, E_8\}$	$B_{15}^{-1} \circ E_8$

This completes the proof of the lemma. □

(IV.14) Theorem. *The groups \mathcal{G} and \mathcal{G}' are the same.*

In other words, the group \mathcal{G} is generated by the following elements:

- (1) $[(A_{2n-2} B_n, A_{2n-1} B_{n-1})]$ for $n \geq 2$ with the convention that $B_1 = A_1$,
- (2) $[(A_{n-2} D_n, A_{n-1} B_{n-1})]$ for $n \geq 4$,
- (3) $[(A_2 B_3, A_3 G_2)]$,
- (4) $[(A_1 B_4 B_6, B_2 B_5 F_4)]$,
- (5) $[(A_4 G_2 A_8 B_6, A_3 A_6 B_5 E_6)]$,

- (6) $[(A_1 B_7 B_9, B_2 B_8 E_7)]$,
 (7) $[(A_1 B_4 B_7 B_{10} B_{12} B_{15}, B_3 B_5 B_8 B_{11} B_{14} E_8)]$.

Proof: Let $[(H_1, H_2)] \in \mathcal{G}$. By theorem (IV.8), the fundamental degrees of the Weyl groups $W(H_1)$ and $W(H_2)$ are the same with the same multiplicities. Let n be the highest fundamental degree of $W(H_1)$ which is the same as the highest fundamental degree of $W(H_2)$. For $i = 1, 2$, let K_i be one of the simple factors of H_i such that n is the highest fundamental degree of $W(K_i)$. Then by previous lemma, there exists an element $[(H'_1, H'_2)] \in \mathcal{G}'$ such that K_i are the simple factors of H'_i and the other simple factors of H'_i have highest fundamental degree less than n . Thus, the element $[(H_1 H'_2, H_2 H'_1)]$ is an element of the group \mathcal{G} and the multiplicity of K_i in either sides of this element is now reduced by 1. This way, we cancel all the simple factors having n as the highest fundamental degree and then the result is obtained by induction. \square

§21. A geometric reasoning.

Here we explain how a transitive action of compact Lie groups is related to the coincidence of orders. The exposition is based on [16, Chapter 2, page 121].

Suppose H is a compact simply connected Lie group acting transitively on a compact manifold $X = H/H_1$ with H_1 connected. Suppose that H_2 is a closed connected Lie subgroup of H and that the action of H on X when restricted to H_2 remains transitive. Then $X = H/H_1 = H_2/(H_1 \cap H_2)$. By looking at the homotopy exact sequence for the fibration $1 \rightarrow H' \rightarrow H \rightarrow H/H' \rightarrow 1$ for any closed subgroup H' of H ,

$$\pi_1(H') \longrightarrow \pi_1(H) \longrightarrow \pi_1(H/H') \longrightarrow \pi_0(H'),$$

we find that H/H' is simply connected if and only if H' is connected. Therefore $X = H/H_1$ is simply connected and hence if $X = H_2/(H_1 \cap H_2)$ with H_2 simply connected, $H_1 \cap H_2$ is connected.

We now assume that there is an analogue of the action of H on X over finite fields, which we now take to be all defined over \mathbb{F}_q . By Lang's theorem (II.4) if H_1 is connected then

$$|(H/H_1)(\mathbb{F}_q)| = \frac{|H(\mathbb{F}_q)|}{|H_1(\mathbb{F}_q)|}.$$

Therefore for the equality of spaces H/H_1 and $H_2/(H_1 \cap H_2)$, with $H_1, H_2, H_1 \cap H_2$ connected, we find that

$$|H(\mathbb{F}_q)| \cdot |(H_1 \cap H_2)(\mathbb{F}_q)| = |H_1(\mathbb{F}_q)| \cdot |H_2(\mathbb{F}_q)|.$$

Thus transitive action of compact Lie groups gives rise to coincidence of orders of finite semisimple groups.

We call an ordered 3-tuple (H, H_1, H_2) , as discussed above, a triple of *inclusion of transitive actions*. We first classify all such triples of inclusion of transitive actions and explain the geometric reasoning behind the order coincidence for the first three pairs described in theorem (IV.14). We note some observations.

(IV.15) Remark. *Let (H, H_1, H_2) be a triple of inclusion of transitive actions, where H , H_1 and H_2 are compact Lie groups such that H_1 is a subgroup of H and the natural action of H_1 on H/H_2 is transitive. Then*

- (1) $H = H_1 H_2$ [16, Lemma 4.1, page 138] and
- (2) *either H_1 or H_2 has the same maximal exponent as the maximal exponent of the group H* [16, Corollary 2, page 143].

(We recall that a natural number a is an exponent of a compact Lie group H if and only if $a + 1$ is a fundamental degree of the Weyl group of H .)

Therefore to classify the inclusions among the transitive actions, equivalently to determine the triples (H, H_1, H_2) of inclusion of transitive actions, it would be desirable to classify the subgroups of a given Lie group of the maximal exponent. We restrict ourselves to the case when H is a simple Lie group.

(IV.16) Theorem (Onishchik, [30]). *Let H be a connected simple compact Lie group and H_1 be a compact Lie subgroup of H having the same maximal exponent as that of H . Then, the pairs $H_1 \subseteq H$ are exhausted by the following list:*

$$\mathrm{Sp}_n \subset \mathrm{SU}_{2n} \ (n > 1), \quad G_2 \subset \mathrm{SO}_7, \quad \mathrm{SO}_{2n-1} \subset \mathrm{SO}_{2n} \ (n > 3),$$

$$\mathrm{Spin}_7 \subset \mathrm{SO}_8, \quad G_2 \subset \mathrm{SO}_8, \quad F_4 \subset E_6.$$

Now, we classify the triples (H, H_1, H_2) , of inclusion of transitive actions, where H is a simple Lie group.

(IV.17) Theorem (Onishchik, [30]). *The triples (H, H_1, H_2) of inclusion of transitive actions where the group H is simple are the following ones:*

H	H_1	H_2	$H_1 \cap H_2$
$\mathrm{SU}_{2n} \ (n \geq 2)$	Sp_n	SU_{2n-1}	Sp_{n-1}
$\mathrm{SO}_{2n} \ (n \geq 4)$	SO_{2n-1}	SU_n	SU_{n-1}
$\mathrm{SO}_{4n} \ (n \geq 2)$	SO_{4n-1}	Sp_n	Sp_{n-1}
SO_7	G_2	SO_6	SU_3
SO_7	G_2	SO_5	SU_2
SO_8	Spin_7	SO_7	G_2
SO_8	Spin_7	SO_6	SU_3
SO_8	Spin_7	SO_5	SU_2
SO_{16}	SO_{15}	Spin_9	Spin_7

Observe that the exponents of the groups $H \times (H_1 \cap H_2)$ and $H_1 \times H_2$ are the same in all above cases. Hence $(H \times (H_1 \cap H_2), H_1 \times H_2)$ is a pair of order coincidence for us. The pairs described in the remark (IV.12) occur in the above descriptions. We can, in fact, give an explicit description of the inclusion among the transitive actions corresponding to the pairs given in the remark (IV.12).

The groups O_n , U_n and Sp_n act on the spaces \mathbb{R}^n , \mathbb{C}^n and \mathbb{H}^n , respectively, in a natural way. By restricting this action to the corresponding spheres, we get that the groups O_n , U_n and Sp_n act transitively on the spheres S^{n-1} , S^{2n-1} and S^{4n-1} , respectively. By fixing a point in each of the spheres, we get the corresponding stabilisers as $O_{n-1} \subset O_n$, $U_{n-1} \subset U_n$ and $Sp_{n-1} \subset Sp_n$.

By treating the space $\mathbb{C}^n = \mathbb{R}^{2n}$, we obtain an inclusion of transitive actions $U_n \subset O_{2n}$, with both the groups acting transitively on S^{2n-1} . Since S^{2n-1} is connected, the actions of $SU_n \subset U_n$ and $SO_{2n} \subset O_{2n}$ on S^{2n-1} remain transitive. Thus we get an inclusion of actions $SU_n \subset SO_{2n}$ and the corresponding stabilisers are $SU_{n-1} \subset SO_{2n-1}$. Thus, we get a triple $(SO_{2n}, SU_n, SO_{2n-1})$ or equivalently we get a pair of order coincidence as $(D_n A_{n-2}, A_{n-1} B_n)$.

Similarly, by treating \mathbb{H}^n as \mathbb{C}^{2n} and repeating the above arguments, we get the inclusion of transitive actions $Sp_n \subset SU_{2n}$, acting on the sphere S^{4n-1} , with $Sp_{n-1} \subset SU_{2n-1}$ as the corresponding stabilisers. This gives us the triple $(SU_{2n}, Sp_n, SU_{2n-1})$ and the pair of order coincidence $(A_{2n-1} B_{n-1}, B_n A_{2n-2})$.

Thus, we get the two infinite families described in the remark (IV.12). The remaining pair of order coincidence, $(A_1 B_3, B_2 G_2)$, can be obtained in a similar way by considering the natural inclusion $G_2 \subset SO_7$. These groups act transitively on the sphere S^6 and the corresponding stabilisers are SU_3 and SO_6 . We observe that SO_6 is isomorphic to SL_4 , therefore the triple (SO_7, G_2, SO_6) gives us $(A_2 B_3, A_3 G_2)$ as the corresponding pair of order coincidence.

Notes.

It would be interesting to know if the pairs (4) to (7) of theorem (IV.14) involving exceptional groups are also obtained in this geometric way.

CHAPTER V

Excellence properties of F_4

This is the last chapter of this thesis. Here we report the work done in [14]. The sections §22, 23 cover the basic material and the last section contains the proof of the main theorem. We also give an easier proof of the main theorem, given by an anonymous referee.

§22. Excellence of linear algebraic groups.

Let G be an algebraic group defined over a field k . We say that G is an *excellent group* if for any extension L of k there exists an algebraic group H defined over k such that $H \otimes_k L$ is isomorphic to the anisotropic kernel of the group $G \otimes_k L$. This notion was introduced by Kersten and Rehmann ([22]) in analogy with the notion of excellence of quadratic forms introduced and studied by Knebusch ([24, 25]). The excellence properties of some groups of classical type have been studied in [20, 22].

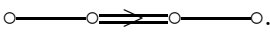
It can be seen that a group of type G_2 is excellent over a field k . Indeed, the group of type G_2 is either anisotropic or it is split ([40, Proposition 17.4.2]). Therefore the anisotropic kernel of this group over any extension is either the whole group or it is trivial, and hence it is always defined over the base field. We prove in this chapter that a group of type F_4 is also excellent over any field of characteristic other than 2 and 3.

Let k be a field of characteristic other than 2 and 3. Let G be a group of type F_4 defined over k and let L be an extension of k . It is known that G can be described as the group of automorphisms of an Albert algebra, \mathcal{A} , defined over k (Theorem I.8). If the split rank of the group $G \otimes_k L$ is 0 or 4, then the respective anisotropic kernels, being either the whole group $G \otimes_k L$ or the trivial subgroup, are defined over k . If the group $G \otimes_k L$ has split rank 1 for an extension L/k , then the corresponding Albert algebra over L can be described as the algebra of 3×3 hermitian matrices over an octonion algebra, say \mathfrak{C} , defined over L . We prove that the anisotropic kernel of the group $G \otimes_k L$ is defined in terms of the norm form of the octonion algebra \mathfrak{C} . Since the octonion algebra \mathfrak{C} is defined over k (cf. [32, Theorem 1.8]), it follows that the anisotropic kernel of $G \otimes_k L$ is defined over k . Thus the group G is an excellent group over k .

§23. Albert algebras and groups of type F_4 .

We fix a field k of characteristic other than 2 and 3 for this section. An *Albert algebra* defined over k is a (non-associative) k -algebra \mathcal{A} such that $\mathcal{A} \otimes_k \bar{k}$ is isomorphic to the split Albert algebra $\mathcal{H}(\mathfrak{C}; \Gamma)$ for the split octonion algebra \mathfrak{C} defined over \bar{k} and for some diagonal $\Gamma \in \mathbb{M}_3(\bar{k})$. These algebras are important because they describe the simple groups of type F_4 and E_6 .

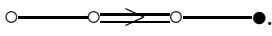
By Tits' classification ([44]), we know that the possibilities for the split ranks of a group of type F_4 are 0, 1 or 4. The anisotropic kernel in each type is the anisotropic group of the type described by the Dynkin diagram obtained by removing the special vertices denoted by \bullet . A group of type F_4 of split rank i is denoted by $F_{4,i}$, for $i = 0, 1, 4$.

The group $F_{4,0}$: 

This group is anisotropic and hence the anisotropic kernel of this group is the group $F_{4,0}$ itself.

The group $F_{4,4}$: 

This group is split, therefore the anisotropic kernel of this group is trivial.

The group $F_{4,1}$: 

This group has a split torus of dimension 1. Once we remove the special vertex from the above Dynkin diagram, we get the Dynkin diagram of type B_3 . Hence the anisotropic kernel of $F_{4,1}$ is an anisotropic group of type B_3 .

We now compute the anisotropic kernel of the group $F_{4,1}$ explicitly. It is known that if the split rank of the k -group $\text{Aut}_k(\mathcal{A})$ is nonzero, then the Albert algebra \mathcal{A} is reduced, i.e., it has an idempotent $\neq 0, 1$. Further, a reduced Albert algebra \mathcal{A} defined over k is k -isomorphic to $\mathcal{H}(\mathfrak{C}; \Gamma)$ for some octonion algebra \mathfrak{C} defined over k and for some diagonal matrix $\Gamma \in \text{GL}_3(k)$ ([40, Theorem 17.6.7]). More precisely, we have

(V.1) Proposition ([1, Theorem 6]). *Let k be a field of characteristic other than 2 and 3, and let G be a group of type F_4 defined over k whose k -rank is 1. Then the group G can be described as the automorphism group of an Albert algebra $\mathcal{A} = \mathcal{H}(\mathfrak{C}; 1, -1, 1)$ where \mathfrak{C} is a division octonion algebra defined over k .*

We fix an Albert algebra $\mathcal{A} = \mathcal{H}(\mathfrak{C}; 1, -1, 1)$ for a division octonion algebra \mathfrak{C} defined over k . Let Q denote the norm form on \mathcal{A} and let $\langle \cdot, \cdot \rangle$ be the associated bilinear form. We denote the group $\text{Aut}_k(\mathcal{A})$ by G , which is a group of type F_4 whose k -rank is 1. To compute G_{an} , we need the description of a maximal torus in G which has a rank 1 split subtorus.

Observe that there is a map $\phi : \text{SO}(1, -1, 1) \rightarrow G$ which sends $X \in \text{SO}(1, -1, 1)$ to the automorphism of \mathcal{A} given by $\theta \mapsto X\theta X^{-1}$ ([31, Lemma 5.1]). The group $\text{SO}(1, -1, 1)$ is a k -split group. Indeed, it contains the following 1-dimensional

split torus,

$$T = \left\{ \begin{pmatrix} a & b & 0 \\ b & a & 0 \\ 0 & 0 & 1 \end{pmatrix} \in \mathrm{GL}_3 : a^2 - b^2 = 1 \right\}.$$

The kernel of the map ϕ is finite, hence the image of the torus T under the map ϕ is a 1-dimensional split torus in G . We prove that this torus $\phi(T)$ can be embedded in a certain subgroup of G of type B_4 and so the anisotropic kernel, G_{an} can be described as the anisotropic kernel of the same subgroup.

(V.2) Lemma. *There exists a primitive idempotent $u \in \mathcal{A}$ such that G_{an} , the anisotropic kernel of the group G , is the same as the anisotropic kernel of the subgroup G_u of G , consisting of those automorphisms of \mathcal{A} that fix u .*

Proof: Define u to be the idempotent

$$\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \in \mathcal{A}.$$

Since $Q(u) := \mathrm{tr}(u^2)/2 = 1/2$, u is a primitive idempotent. Let G_u denote the subgroup of G consisting of the automorphisms of \mathcal{A} which fix u . This subgroup G_u is isomorphic to the group $\mathrm{Spin}(Q, E_0)$ ([40, Proposition 7.1.6]), where

$$E_0 := \{x \in \mathcal{A} : \langle x, 1 \rangle = \langle x, u \rangle = 0, ux = 0\}.$$

It can be easily seen that the space E_0 is given by:

$$E_0 = \left\{ \begin{pmatrix} x & c & 0 \\ -\bar{c} & -x & 0 \\ 0 & 0 & 0 \end{pmatrix} \in \mathcal{A} \right\} \xrightarrow{\sim} k \oplus \mathfrak{C}.$$

Thus, the space E_0 is a 9-dimensional vector space over k and hence the group $\mathrm{Spin}(Q, E_0)$ is a group of type B_4 . The quadratic form on E_0 is given by

$$(x, c) \mapsto x^2 - c\bar{c} = x^2 - N(c),$$

where N denotes the norm form of \mathfrak{C} . It can be seen that the torus $\phi(T)$ fixes the idempotent u , therefore $\phi(T)$ is contained in G_u . It is a group of k -rank 1, as it contains the torus $\phi(T)$. By Tits classification ([44, page 55, 56]), we know that the anisotropic kernel of G_u is a group of type B_3 . Moreover, G_{an} is also a group of type B_3 and it contains $(G_u)_{an}$, therefore it is clear that the anisotropic kernels of the groups G and G_u are the same. \square

§24. The main theorem.

This section is devoted to the proof of the following main theorem.

(V.3) Theorem. *Let k be a field of characteristic other than 2 and 3 and let G be a group of type F_4 defined over k . Then G is an excellent group.*

Proof: Let k be a field of characteristic other than 2 and 3 and fix a simple group G of type F_4 defined over k . Let \mathcal{A} be the Albert algebra such that $G = \text{Aut}_k(\mathcal{A})$. We want to show that for any extension L/k , there exists a group H defined over k such that $H \otimes_k L$ is isomorphic to $(G \otimes_k L)_{an}$. Fix an extension L/k .

If the L -rank of the group $G \otimes_k L$ is 0, we define H to be the group G itself and if the L -rank of $G \otimes_k L$ is 4, then we define H to be the trivial subgroup of G .

Now, let the L -rank of the group $G \otimes_k L$ be 1. Then the group $G \otimes_k L$ can be described as the group of L -automorphisms of the Albert algebra $\mathcal{H}(\mathfrak{C}; 1, -1, 1)$ for some division octonion algebra \mathfrak{C}/L . By the uniqueness of the Albert algebra, we have $\mathcal{A} \otimes_k L \xrightarrow{\sim} \mathcal{H}(\mathfrak{C}; 1, -1, 1)$. By lemma (V.2), the anisotropic kernel of the group $G \otimes_k L$ is the same as that of a subgroup of type B_4 which is isomorphic to $\text{Spin}(Q, L \oplus \mathfrak{C})$, where the form Q is given by

$$(l, c) \mapsto l^2 - N(c)$$

where N is the norm form of the division octonion algebra \mathfrak{C} .

It is a theorem of Serre and Rost that for an Albert algebra defined over k and for a reducing field extension L/k , the co-ordinate octonion algebra is defined over k ([32, Theorem 1.8]).

Therefore, the algebra \mathfrak{C} is defined over k and so is the norm form N . Hence the quadratic form Q is also defined over k . We define H to be the anisotropic kernel of the k -group $\text{Spin}(Q, k \oplus \mathfrak{C})$, then it is clear that $H \otimes_k L$ is isomorphic to the anisotropic kernel of $G \otimes_k L$.

Thus the group G is an excellent group. □

Notes.

In §23, we compute the anisotropic kernel of any group of type F_4 defined over k . These computations are important for the proof presented in the last section. Now, we give a proof which does not require these computations.

Another proof of Theorem (V.3). Let k be a field of characteristic other than 2 and 3, and let G be a group of type F_4 defined over k . Let G be isomorphic to $\text{Aut}_k(\mathcal{A})$ for an Albert algebra \mathcal{A}/k . Let L be an extension of k .

If the split rank of the group $G \otimes_k L$ is 0 or 4, then the anisotropic kernel of the group $G \otimes_k L$ is clearly defined over k .

If the split rank of the group $G \otimes_k L$ is 1, then $G \otimes_k L \xrightarrow{\sim} \text{Aut}_L(\mathcal{A} \otimes_k L)$ where $\mathcal{A} \otimes_k L$ is a reduced Albert algebra defined over L . Then there exists an octonion algebra \mathfrak{C} defined over L such that $\mathcal{A} \otimes_k L \xrightarrow{\sim} \mathcal{H}(\mathfrak{C}; 1, -1, 1)$. By the theorem of Serre and Rost ([32, Theorem 1.8]), the octonion algebra \mathfrak{C} is defined over k . Define G' to be the k -automorphism group of the k -algebra $\mathcal{H}(\mathfrak{C}; 1, -1, 1)$. Then G' is a group of type F_4 and its k -rank is 1. Clearly, the anisotropic kernel of the group G' is isomorphic to $(G \otimes_k L)_{an}$ over L and hence the anisotropic kernel of the group $G \otimes_k L$ is defined over k .

This proves that the group G is excellent. □

Bibliography

- [1] **Adrian A. Albert; Nathan Jacobson:** *On reduced exceptional simple Jordan algebras*, Annals of Math., **66**, (1957), 400–417.
- [2] **Emil Artin:** *The orders of the linear groups*, Comm. Pure Appl. Math., **8**, (1955), 355–365.
- [3] **Emil Artin:** *The orders of the classical simple groups*, Comm. Pure Appl. Math., **8**, (1955), 455–472.
- [4] **Armand Borel:** *Linear algebraic groups*, Graduate Texts in Mathematics, **126**, Springer-Verlag, New York, (1991).
- [5] **Armand Borel; Tonny A. Springer:** *Rationality properties of linear algebraic groups II*, Tohoku Math. J. (2), **20**, 443–497 (1968).
- [6] **Nicolas Bourbaki:** *Lie groups and Lie algebras*, Chapters 4–6, translated from the 1968 French original, Elements of Mathematics (Berlin), Springer-Verlag, Berlin, (2002).
- [7] **Francois Bruhat; Jacques Tits:** *BN-paires de type affine et données radicielles*, C. R. Acad. Sci. Paris, Sér. A-B, **263**, A598–A601, (1966).
- [8] **Francois Bruhat; Jacques Tits:** *Groupes simples résiduellement déployés sur un corps local*, C. R. Acad. Sci. Paris, Sér. A-B, **263**, A766–A768, (1966).
- [9] **Francois Bruhat; Jacques Tits:** *Groupes algébriques simples sur un corps local*, C. R. Acad. Sci. Paris, Sér. A-B, **263**, A822–A825, (1966).
- [10] **Francois Bruhat; Jacques Tits:** *Groupes algébriques simples sur un corps local: Cohomologie galoisienne, décompositions d'Iwasawa et de Cartan*, C. R. Acad. Sci. Paris, Sér. A-B, **263**, A867–A869, (1966).
- [11] **J. W. S. Cassels; A. Frohlich:** *Algebraic number theory*, (Proceedings of the instructional conference held at the University of Sussex, Brighton, September 1–17, 1965), Academic Press, Inc., (1986).
- [12] **Shripad M. Garge:** *Maximal tori determining the algebraic group*, to appear in Pac. Jour. of Math.
- [13] **Shripad M. Garge:** *On the orders of finite semisimple groups*, preprint.
- [14] **Shripad M. Garge:** *Excellence properties of F_4* , preprint.
- [15] **Philippe Gille:** *Type des tores maximaux des groupes semisimples*, to appear
- [16] **Vladimir V. Gorbatsevich, Arkadi L. Onishchik, Ernest B. Vinberg,** *Foundations of Lie theory and Lie transformation groups*, [Lie groups and Lie algebras: I, Encyclopedia Math. Sci., **20**, Springer, Berlin, (1993)]. Springer-Verlag, Berlin, (1997).
- [17] **Hiroaki Hijikata:** *A remark on the groups of type G_2 and F_4* , J. Math. Soc. Japan, **15**, 159–164, (1963).
- [18] **James E. Humphreys:** *Linear algebraic groups*, Graduate Texts in Mathematics, **21**, Springer-Verlag, New York-Heidelberg, (1975).
- [19] **James E. Humphreys:** *Reflection groups and Coxeter groups*, Cambridge Studies in Advanced Mathematics, **29**, Cambridge University Press, Cambridge (1990).

- [20] **Oleg H. Izhboldin; Ina Kersten:** *Excellent special orthogonal groups*, Doc. Math., **6** (2001), 385–412.
(available electronically at <http://www.math.uiuc.edu/documenta/vol-06/>)
- [21] **Kazutoshi Kariyama:** *On conjugacy classes of maximal tori in classical groups*, J. Algebra, **125**, 133–149 (1989).
- [22] **Ina Kersten; Ulf Rehmann:** *Excellent algebraic groups I*, Journal of Algebra, **200**, (1998), 334–346.
- [23] **Wolfgang Kimmerle, Richard Lyons, Robert Sandling, David Teague:** *Composition factors from the group ring and Artin’s theorem on orders of simple groups*, Proc. London Math. Soc. (3), **60**, (1990), 89–122.
- [24] **Manfred Knebusch:** *Generic splitting of quadratic forms I*, Proc. London Math. Soc. (3), **33**, (1976), 65–93.
- [25] **Manfred Knebusch:** *Generic splitting of quadratic forms II*, Proc. London Math. Soc. (3), **34**, (1977), 1–31.
- [26] **Martin Kneser:** *Galois-kohomologie halbenfacher algebraischer Gruppen über p -adischen Körpern I*, Math. Z. **88**, 40–47 (1965).
- [27] **Martin Kneser:** *Galois-kohomologie halbenfacher algebraischer Gruppen über p -adischen Körpern II*, Math. Z. **89**, 250–272 (1965).
- [28] **Max-Albert Knus; Alexander Merkurjev; Markus Rost; Jean-Pierre Tignol:** *The Book of Involutions*, Colloquium Publications, **44**, American Mathematical Society, Providence, RI (1998).
- [29] **Serge Lang:** *Algebraic groups over finite fields*, Amre. J. Math. **78**, 553–563 (1958).
- [30] **Arkadi L. Onishchik:** *Inclusion relations between transitive compact transformation groups*, Tr. Mosk. Mat. O-va, **11**, (1962), 199–242.
English translation: Transl. II. Ser., Amer. Math. Soc., **50**, (1966), 5–58.
- [31] **R. Parimala; V. Suresh; Maneesh Thakur:** *Jordan algebras and F_4 bundles over the affine plane*, Journal of Algebra, **198**, (1997), 582–607.
- [32] **Holger P. Petersson; Michel L. Racine:** *On the invariants mod 2 of Albert algebras*, Journal of Algebra, **174**, (1995), 1049–1072.
- [33] **Richard S. Pierce:** *Associative Algebras*, Graduate Texts in Mathematics, **88**, Springer-Verlag, New York-Heidelberg-Berlin (1982).
- [34] **Vladimir Platonov; Andrei Rapinchuk:** *Algebraic Groups and Number Theory*, Pure and Applied Mathematics, **139**, Academic Press, Inc., CA (1994).
- [35] **Jean-Pierre Serre:** *Local Fields*, Graduate Texts in Mathematics, **67**, Springer-Verlag, New York Inc. (1979).
- [36] **Jean-Pierre Serre:** *Galois cohomology*, Corrected reprint of the 1997 English edition, Springer Monographs in Mathematics, Springer-Verlag, Berlin, (2002).
- [37] **Tonny A. Springer:** *Galois cohomology of linear algebraic groups*, Algebraic Groups and Discontinuous Subgroups (Proc. Sympos. Pure Math., Boulder, Colo., 1965), **IX**, Amer. Math. Soc., (1966), 149–158.
- [38] **Tonny A. Springer:** *Regular elements of finite reflection groups*, Invent. Math., **25**, 159–198 (1974).
- [39] **Tonny A. Springer:** *Linear algebraic groups*, Second edition, Progress in Mathematics, **9**, Birkhuser Boston, Inc., Boston, MA, (1998).
- [40] **Tonny A. Springer; Ferdinand D. Veldkamp:** *Octonions, Jordan algebras and exceptional groups*, Springer monographs in Mathematics, Springer-Verlag Berlin Heidelberg, (2000).

- [41] **Jacques Tits:** *Sur la trialité et certains groupes qui s'en déduisent*, Inst. Hautes Études Sci. Publ. Math., **2**, (1959), 13–60.
- [42] **Jacques Tits:** *Groupes simples et géométries associées*, Proc. Internat. Congr. Mathematicians (Stockholm, 1962), (1963), 197–221.
- [43] **Jacques Tits:** *Algebraic and abstract simple groups*, Ann. of Math., **80**, (1964), 313–329.
- [44] **Jacques Tits:** *Classification of algebraic semisimple groups*, Algebraic Groups and Discontinuous Subgroups (Proc. Sympos. Pure Math., Boulder, Colo., 1965), **IX**, Amer. Math. Soc., (1966), 33–62
- [45] **Jacques Tits:** *Normalisateurs de Tores I. Groupes de Coxeter Etendus*, J. Algebra, **4**, 96–116 (1966).
- [46] **Jacques Tits:** *Théorie des groupes*, Résumé des Cours de 1976 – 1977, (1978), 57–67.
- [47] **Jacques Tits:** *Les “formes réelles” des groupes de type E_6* , Séminaire Bourbaki, **4**, Exp. No. 162, Soc. Math. France, Paris, (1995), 351–365.
- [48] **Jacques Tits:** *Les groupes simples de Suzuki et de Ree*, Séminaire Bourbaki, **6**, Exp. No. 210, Soc. Math. France, Paris, (1995), 65–82.

Index

- 1-cocycle, 22
- k -group, 9
- k -rank, 13
- k -split torus, 12
- k -torus, 12
- p -contribution, 48

- adjoint algebraic group, 12
- Albert algebra, 20
- anisotropic algebraic group, 13
- anisotropic kernel, 14
- anisotropic octonion algebra, 19
- arithmetic field, 29

- central isogeny, 12
- composition algebra, 18

- derived group, 11
- Dynkin diagram, 15

- excellent algebraic group, 67

- fundamental degrees, 34

- general linear group, 10

- inclusion of transitive actions, 65
- isogeny, 9
- isotropic algebraic group, 13

- linear algebraic group, 9

- maximal k -split torus, 13
- maximal torus, 13

- neutral element in H^1 , 22
- norm form, 18

- octonion algebra, 19

- pair of order coincidence, 57
- pointed set, 22

- radical, 11
- rank, 13
- reductive algebraic group, 11
- root system, 15
- roots, 14

- semisimple algebraic group, 11
- simple algebraic group, 11
- simple direct factors, 12
- simple roots, 15
- simple Weyl group, 30
- simply connected algebraic group, 12
- split Albert algebra, 20
- split octonion algebra, 19
- split reductive group, 13
- split torus, 13

- torus, 12

- unipotent algebraic group, 11
- unipotent radical, 11

- Weyl group, 13

Notation

(G, G) , 11	SO_n , 16
A^G , 21	Sp_n , 10
$ch(W)$, 34	$W(G)$, 13
$ch^*(W)$, 34	$Z^1(G, A)$, 21
$D(G)$, 15	
G° , 10	
G_{an} , 14	
GL_n , 10	
\mathbb{G}_m , 10	
$H^0(G, A)$, 21	
$H^1(G, A)$, 21	
$H^i(G, A)$, 21	
$H^i(k, G)$, 22	
$\mathcal{H}(\mathfrak{C}; \Gamma)$, 19	
$\mathcal{H}(\mathfrak{C}; \gamma_1, \gamma_2, \gamma_3)$, 19	
$\mathfrak{m}'_i(W)$, 34	
$\mathfrak{m}_i(W)$, 34	
$\mathfrak{m}_{i,j}(W)$, 34	
O_n , 10	
$\mathrm{ord}_p m$, 48	
$\Phi(G)$, 14	
$\Phi_n(x, y)$, 48	
$\Pi(G)$, 15	
$\phi_n(x)$, 48	
ϕ_r , 34	
$R(G)$, 11	
$R_u(G)$, 11	
SL_n , 10	